● 国家出版基金资助项目

中国科学院华罗庚数学重点实验室丛书

华罗庚文集

代数卷 I

华罗庚 万哲先 / 著

万哲先 / 审校

科学出版社
www.sciencep.com

国家出版基金资助项目

中国科学院华罗庚数学重点实验室丛书

华罗庚文集

代数卷 I

华罗庚　万哲先　著

万哲先　审校

科 学 出 版 社

北　京

内 容 简 介

本卷是典型群方面作者历年来工作的系统总结性论著，也包含了作者在体论和矩阵几何方面的工作．书中不仅列举了作者在这一领域中所获得的丰富而完整的结果，也充分体现了作者所创用的方法和技巧的特点．

全卷共分十二章，前六章由第一作者执笔，初稿完成于 1951 年，后六章由第二作者根据他所体会的前六章的精神和方法续写．书末附有一些注释．

本卷适合数学及相关专业大学生、研究生、教授及科研人员阅读参考．

图书在版编目（CIP）数据

华罗庚文集：代数卷 I/华罗庚，万哲先著；万哲先审校．—北京：科学出版社，2010

（中国科学院华罗庚数学重点实验室丛书）

ISBN 978-7-03-027126-6

Ⅰ. 典… Ⅱ. ①华…②万… Ⅲ. ①数学-文集…②代数-文集 Ⅳ. 01-53

中国版本图书馆 CIP 数据核字(2010) 第 056713 号

科学出版社 出版
北京东黄城根北街 16 号
邮政编码：100717
http://www.sciencep.com

中国科学院印刷厂 印刷

科学出版社发行 各地新华书店经销

*

2010 年 5 月第 一 版 开本：B5(720×1000)
2010 年 5 月第二次印刷 印张：32
印数：1—3 000 字数：628 000

定价：98.00 元

（如有印装质量问题，我社负责调换）

《华罗庚文集》序言

2010 年是著名数学家华罗庚先生诞辰 100 周年. 值此机会, 我们编辑出版《华罗庚文集》, 作为对他的美好纪念.

华罗庚先生是他那个时代的国际领袖数学家之一, 也是中国现代数学的主要奠基人和领导者. 无论是在和平建设时期, 还是在政治动荡甚至是战争年代, 他都抱定了为国家和人民服务的宗旨, 为中国数学的发展倾注了毕生精力, 受到了中国人民的广泛尊敬.

华罗庚先生最初研究数论, 后将研究兴趣拓展至代数和多复变等多个领域, 取得了一系列国际一流的成果, 引领了这些领域的学术发展, 产生了广泛持久的影响. 他从一名自学青年成长为著名数学家, 其传奇经历激励了几代中国数学家投身于数学事业.

华罗庚先生为我们留下了丰富的精神遗产, 包括大量的学术著作和研究论文. 我们认为, 认真研读这些著作和论文, 是深刻把握华罗庚学术思想精髓的最佳途径. 无论对于数学工作者还是青年学生, 其中许多内容都是很有启发和裨益的.

华罗庚先生担任中国科学院数学研究所所长 30 余年, 他言传身教, 培养和影响了一批国际水平的数学家, 他的学术思想和治学精神已经成为数学所文化的核心. 自 2008 年起以中科院数学所为基础成立的中国科学院华罗庚数学重点实验室, 旨在继承和弘扬华罗庚先生的学术思想和治学精神, 积极推动中国数学的发展. 为此, 我们选择华罗庚先生的著作和论文作为实验室的首批出版物, 今后还将陆续推出更多优秀的数学出版物.

在出版《华罗庚文集》的过程中, 我们得到了各方面的关心和支持, 包括国家出版基金的资助, 在此我们表示深深的感谢. 同时, 对于有关人员在策划、翻译和审校等方面付出的辛勤劳动, 对于科学出版社所作的大量工作, 我们表示诚挚的谢意.

中国科学院华罗庚数学重点实验室

《华罗庚文集》编委会

2010 年 3 月

序[1]

早在 1949 年, 本书作者之一就有了写这样一本书的轮廓, 希望根据这个轮廓组织一个讨论班, 和一批大学四年级及刚毕业的同学在一起, 使他们边学习边搞研究, 集体地较整套地来进行这一领域的研究工作, 一来可以使他们在工作过程中逐步地扩充自己的知识领域, 另一方面可以让他们习作一些研究, 预计在计划完成之后, 可以给典型群论, 射影几何学, 矩阵论及群表示论等数学分支以一个不同的面貌. 1950 年初, 当他在北京清华大学执教时, 组织了这样一个讨论班. 讨论班进行到 1951 年暑假, 在讨论班里他完成了本书前六章的初稿. 接着, 在 1951 年下半年和 1957 年上半年, 他又在中国科学院数学研究所代数讨论班里两度报告了本书前六章的大部分章节, 并进行了一些修改. 随后, 从 1959 年下半年起, 本书后一作者又在数学研究所代数讨论班里报告了前六章的部分章节, 并根据他所体会的前六章的精神与方法续写了本书的后六章. 这就是本书简单的写作经过.

简要地可以这样说, 体上的矩阵是一个值得注意的对象, 因为它是一个不太失去普遍性的抽象事物, 但同时又和成果丰富的具体的域上的矩阵论距离不远. 当然, 结合环, 李环和柔丹环中有趣的部分又都有矩阵形式, 而线性群, 正交群, 辛群, 洛伦兹群也都是矩阵群; 几何学中线几何, 圆几何, 格拉斯曼几何都有矩阵的表示法. 更如多复变函数论的典型域也离不开矩阵的表达形式. 这些形成了我们的工作背景.

仅仅找到一个值得研究的对象, 而没有处理的方法那也还是空话. 本书中提供了一些方法, 这些方法是初步的, 有待改进, 补充和发展, 只有在发展过程中才能把方法搞得更完备.

1950 年本书作者之一选择这个主题的原因之一是为了易于训练干部. 预备知识需要得少, 可以从简单处着手, 从具体处着手; 发展前途不太小, 通过这一系列的研究也可以熟悉代数学, 几何学中不少分支, 可以从宽广处着眼, 从抽象处着眼. 换言之, 开始时不受基础的限制, 终了时不致局促于太仄狭的领域之中.

匆匆已经十年, 这计划还只能说在第一阶段中完成了第一部分而已. 更重要的工作还有待于今后的努力. 这决不是一个完整的东西, 而仅仅是一个开始. 这是一个阶梯中的一级, 读者必须想想前面几级 —— 实数域, 复数域, 有限域及四元数体上的情况, 读者更必须看看后面几级 —— 体上矩阵的环和群的构造, 不用连续性

---

[1] 本卷内容曾作为著作出版, 见《典型群》, 北京科学出版社, 1963.

的群表示论等等, 这样才不致于为本书引入歧途. 长期局限于本书范围内的工作将不是作者的本意, 但我们认为搞清这些对象和方法对学好典型群论, 射影几何学等都能有所帮助.

我们感谢王仰贤, 应玫茜, 徐诚浩等同志, 在本书付印之前, 他们分头阅读了本书手稿的各部分, 进行了核算, 并提出了一系列宝贵的修改意见.

华罗庚　万哲先

1962 年 8 月于北京

目　　录

第一章 体 论

§1 环 与 体

为了使本书尽可能地自给自足，我们先叙述一下环和体的基本性质，并且提供若干例子，通过这些例子来说明某些概念的具体涵义.

定义 1 环 R 乃具有两种运算"+"及"×"的集合，即若 a, b 在 R 中，则 $a+b$ 及 $a\times b$ 也是 R 中唯一定义的元素；这两个运算有以下性质：

I. 对加运算"+"，R 成一交换群 (或称为 Abel 群)，即对 R 中的任意三元素 a, b, c 有次之关系：(i) $a+b=b+a$; (ii) $(a+b)+c=a+(b+c)$; (iii) R 有一元素 0，称为零元素，使对所有的 a，常有 $0+a=a$，及 (iv) 对 R 中任意元素 a，R 中一定有一个元素 b，使得 $a+b=0$;

II. 对乘运算"×"，适合结合律，即对 R 中的任意三元素 a, b, c，常有

$$(a\times b)\times c=a\times(b\times c);$$

III. 加乘之间适合分配律，即对 R 中的任意三元素 a, b, c，常有

$$a\times(b+c)=a\times b+a\times c,$$
$$(b+c)\times a=b\times a+c\times a.$$

以后为方便计，将"×"号略去，通常习见的名词"和"，"差"，"积"等名词，其义自明，不再定义.

〔例 1〕 所有的整数成一环；所有的偶数也成一环.

〔例 2〕 命 m 表一正整数，以 m 为模所得的同余类成一环. 且看一个具体情形. 命 $m=6$，任一整数可以唯一地归入下面六类之一：

$$\{0+6k\},\quad \{1+6k\},\quad \{2+6k\},\quad \{3+6k\},\quad \{4+6k\},\quad \{5+6k\}.$$

分别以 $\Gamma_0,\cdots,\Gamma_5$ 表示上述的类. 两类的加法定义为

$$\Gamma_i+\Gamma_j=\Gamma_k, 若 i+j\equiv k \pmod 6,$$

而 Γ_0 为加法群中的零元素；乘法定义为

$$\Gamma_i\Gamma_j=\Gamma_k, 若 ij\equiv k \pmod 6.$$

显然, 这样定义出一个环.

〔**例 3**〕　所有带有理系数的单变数多项式成一环.

〔**例 4**〕　以一多项式为模, 分上例中所述的多项式为同余类, 这些类也成为一环.

〔**例 5**〕　形如 $a+bi$ ($i=\sqrt{-1}$) 的数, 其中 a,b 为整数, 也成一环.

〔**例 6**〕　所有在区间 (a,b) 内的连续函数成一环.

〔**例 7**〕　复变数函数论中所讨论的全体整函数也成一环.

环 R 中的零元素 0 还有次之性质: 由

$$0a=(0+0)a=0a+0a$$

可知

$$0a=0.$$

同样, 可知 $a0=0$. 即 0 左乘或右乘任一元素恒为 0. 但从 $ab=0$ 并不能断定 a,b 中至少有一为 0; 例如, 在例 2 中, $\Gamma_2\Gamma_3=\Gamma_0$, 但是 $\Gamma_2\neq\Gamma_0,\Gamma_3\neq\Gamma_0$. 因而我们定义: 环中如有二元素 $a\neq 0,b\neq 0$ 而 $ab=0$, 则称 a 为左零因子, b 为右零因子.

显然, 如果环中无左零因子, 当然也无右零因子. 这样的环谓之无零因子的环.

如果环 R 的一个子集合 S 对 R 的两个运算也成一环, 那么, S 称为环 R 的子环. 例 1 即说明子环是存在的.

定义 2　环 R 若再满足下面的条件则称为体:

II′. R 中除 0 外, 其他的元素对乘法成一群, 即有一元素 1, 称为么元素, 使 $1\cdot a=a$, 而且对 R 中任意元素 $a\neq 0$, 有一元素 b 存在, 使 $b\cdot a=1$.

若体中乘法满足交换律, 即 $ab=ba$, 则体称为域.

〔**例 1**〕　命 p 为一素数, 以 p 为模所得的同余类成一域.

〔**例 2**〕　所有的有理数成一域.

〔**例 3**〕　所有的形如 $a+bi$ 的数也成一域, 此处 a,b 过所有的实数.

〔**例 4**〕　所有的有理函数成一域.

〔**例 5**〕　所有的半纯函数也成一域.

以上列举的全是域的例子. 现在问: 是否有非域之体?

〔**例 6**〕　命 F 表一实域, 就是具有下述性质的域: 如果若干个元素的平方的和等于 0, 则这些元素全是 0. 命 i,j,k 为三元素, 与 F 中的元素皆可交换, 且具有以下诸性质:

$$ij=-ji=k,\quad jk=-kj=i,\quad ki=-ik=j,$$

(1)

$$i^2=j^2=k^2=-1.$$

我们考虑全体形如

$$a_0 + a_1 i + a_2 j + a_3 k \quad (a_0, a_1, a_2, a_3 \in F)$$

的元素. 这种元素称为四元数, 以 Q 表所有的四元数所成的集合, 其中的加法定义为

$$\begin{aligned}&(a_0 + a_1 i + a_2 j + a_3 k) + (b_0 + b_1 i + b_2 j + b_3 k)\\ =\,&(a_0 + b_0) + (a_1 + b_1)i + (a_2 + b_2)j + (a_3 + b_3)k,\end{aligned}$$

其乘法由 (1) 式及分配律予以确定. 读者试自验证, Q 是一体, 称为四元数体.

易见, 在 Q 中与任一元素皆可交换的元素所成的集合, 就是 F. 这一性质引出以下概念:

一体 R 中的元素 a, 若对所有的 $x \in R$ 常满足

$$ax = xa,$$

则 a 称为 R 的中心元素. 全体中心元素所成的集合, 称为 R 的中心. 显然中心成一域.

一体的子集, 如果对体的原有的两种运算仍成一体, 这子集称为原体的子体, 而称原体为子体的扩体. 例 6 中的 F 是 Q 的子体.

〔**例 7**〕 命 F 为一域, 系数在 F 中所有的 x 的多项式成一环, 以 $F[x]$ 记之. 设 $f(x)$ 为系数在 F 中的不可分解的多项式. 以 $f(x)$ 为模, 分多项式为若干类, 如此诸类成一域, 证明如下:

对任一 $g(x)$, 如非 $f(x)$ 的倍数, 由辗转相除法可得二多项式 $a(x)$ 与 $b(x)$, 使

$$a(x)g(x) + b(x)f(x) = 1,$$

此处 $a(x)$, $b(x)$ 的系数也在 F 中. 由此立得

$$a(x)g(x) \equiv 1 \pmod{f(x)}.$$

即 $g(x)$ 所代表的同余类以 $a(x)$ 所代表的同余类为其逆. 显然可见, 此域以 F 为其子域.

假定 α 是方程式 $f(x) = 0$ 的根, 且 α 与 F 中的元素都可交换, 则形如

$$a_0 + a_1\alpha + \cdots + a_{n-1}\alpha^{n-1} \quad (a_0, \cdots, a_{n-1} \in F)$$

之元素成一域, 此处 n 为多项式 $f(x)$ 的次数. 只须重复上面的讨论就可以证明这一性质. 如此所得的域称为 F 的单代数扩域, 且以符号 $F(\alpha)$ 记之.

§2　特征数及素域, 由环建体

设 R 为一无零因子的环. 对 R 中某一元素 $a \neq 0$, 若有最小正整数 p 存在, 使 $pa = 0$, 即

$$\underbrace{a + a + \cdots + a}_{p \text{ 个}} = 0,$$

则 p 称为此环的特征数. 若不存在这样的 p, 则称此环为特征数为零的环, 或记之以 $p = 0$. 特征数 p 有下述的性质:

I. p 与 a 的选择无关;

II. p 为素数.

事实上, 设 $a \neq 0$, $b \neq 0$ $(a, b \in R)$, 则由

$$(pa)b = a(pb)$$

可知由 $pa = 0$ 推出 $pb = 0$. 反之, 由 $pb = 0$ 推得 $pa = 0$, 故得 I.

又若 p 不是素数而 $p = p_1 p_2$ $(p_1 > 1, p_2 > 1)$, 则 $pa = p_1(p_2 a) = 0$, 若 $p_2 a = 0$, 此与 p 的假设不合; 若 $p_2 a \neq 0$, 此与 I 相矛盾, 故得 II.

命 R 为有么元素的环, Σ 为 R 中包含么元素的最小子环. 若 R 为无零因子环而且 R 之特征数是 p, 则 Σ 就是: $0, 1, \cdots, p-1$ 所构成的集合. 若 R 之特征数为 0, 则 Σ 就是所有的整数.

命 F 为一体, 若 F 的特征数是 p, 则 F 的最小子体就是由 $0, 1, \cdots, p-1$ 这些元素所构成的域. 若特征数是 0, 则 F 的最小子体就是由全体有理数所组成的域. 这最小子体称为体 F 的素域.

定义 1　在一环中, 如 $a = bc$, 则 b 称为 a 的左因子, c 称为 a 的右因子; a 称为 b 的右倍数, c 的左倍数. 若有一元 m 具有性质

$$m = aa_1 = bb_1,$$

则 m 称为 a 及 b 的右公倍数. 显然可以类似地定义任意多个元素的右公倍数.

本节之目的在于: 从无零因子而任二元素有右公倍数的环出发, 仿照由整数建立有理数的方法, 来建立体.

为了这个目的, 我们将下面的集合分类:

$$\{(a, b); a, b \in R, b \neq 0\}.$$

设有 (a, b), (c, d). 若对于 d, b 的某一右公倍数 $m = bb_1 = dd_1, ab_1 = cd_1$ 成立, 则称 (a, b) 与 (c, d) 属于同类, 以 $(a, b) \sim (c, d)$ 表之.

首先证明, 此定义与 m 的选择无关. 即若 m' 为另一右公倍数, $m' = bb'_1 = dd'_1$, 则我们仍有 $ab'_1 = cd'_1$. 事实上, 由假定, m 与 m' 有一右公倍数 $M = mx = m'y$, 则有 $b_1x = b'_1y$ 及 $d_1x = d'_1y$. 再由 $ab_1 = cd_1$ 立得 $ab'_1y = ab_1x = cd_1x = cd'_1y$, 即 $ab'_1 = cd'_1$.

其次证明: 关系 "$\sim$" 是一等价关系, 即有以下的三种性质:

1. 反身性 $(a, b) \sim (a, b)$;
2. 对称性 若$(a, b) \sim (c, d)$, 则 $(c, d) \sim (a, b)$;
3. 传递性 若$(a, b) \sim (c, d), (c, d) \sim (e, f)$, 则 $(a, b) \sim (e, f)$.

1 及 2 是显然的事实. 现在我们去证明传递性. 易见任何三元素 b, d, f, 必有一右公倍数 m 使

$$m = bb_1 = dd_1 = ff_1,$$

由假定 $ab_1 = cd_1, cd_1 = ef_1$, 故得 $ab_1 = ef_1$, 即 $(a, b) \sim (e, f)$.

所有的类成一集合, 以 K 表之. 今以 $\dfrac{a}{b}$ 表示 (a, b) 所属之类, (a, b) 称为此类的代表. 今在 K 中定义加法和乘法.

对于加法, 我们作如下的定义:

$$\frac{a}{b} + \frac{c}{d} = \frac{ab_1 + cd_1}{m},$$

此处 m 是 b 及 d 的一个右公倍数, 且 $m = bb_1 = dd_1$.

首先指出这定义与 m 的选择无关. 盖设 $m' = bb'_1 = dd'_1$ 及 $M = mx = m'y$, 则 $b_1x = b'_1y, d_1x = d'_1y$, 故得

$$\begin{aligned}\frac{a}{b} + \frac{c}{d} &= \frac{ab_1 + cd_1}{m} = \frac{ab_1x + cd_1x}{mx} \\ &= \frac{ab'_1y + cd'_1y}{m'y} = \frac{ab'_1 + cd'_1}{m'}.\end{aligned}$$

其次指出, 此定义与 $\dfrac{a}{b}$ 及 $\dfrac{c}{d}$ 的代表选择无关.

设 $\dfrac{a}{b} = \dfrac{a'}{b'}, \dfrac{c}{d} = \dfrac{c'}{d'}$, 则 $m = bb_1 = b'b'_1 = dd_1 = d'd'_1$, 由假定知 $ab_1 = a'b'_1, cd_1 = c'd'_1$, 故得

$$\frac{a}{b} + \frac{c}{d} = \frac{ab_1 + cd_1}{m} = \frac{a'b'_1 + c'd'_1}{m} = \frac{a'}{b'} + \frac{c'}{d'}.$$

对于乘法定义如下:

$$\left(\frac{a}{b}\right)\left(\frac{c}{d}\right) = \frac{ab_1}{dc_1},$$

此处 $m = bb_1 = cc_1$, 而 $b \neq 0, c \neq 0$.

同样可证, 此定义与 m 的选择无关. 设 $m' = bb_1' = cc_1', mx = m'y$, 则 $b_1x = b_1'y, c_1x = c_1'y$, 故得

$$\left(\frac{a}{b}\right)\left(\frac{c}{d}\right) = \frac{ab_1}{dc_1} = \frac{ab_1x}{dc_1x} = \frac{ab_1'y}{dc_1'y} = \frac{ab_1'}{dc_1'}.$$

再证明此定义与 $\frac{a}{b}$ 及 $\frac{c}{d}$ 的代表选择无关. 若 $\frac{a}{b} = \frac{a'}{b'}, \frac{c}{d} = \frac{c'}{d'}$, 由此可设

$$bb_1 = b'b_1', \quad ab_1 = a'b_1'; \quad dd_1 = d'd_1', \quad cd_1 = c'd_1'.$$

取 $m = bb_1\alpha = b'b_1'\alpha = cd_1\beta = c'd_1'\beta$, 故

$$\left(\frac{a}{b}\right)\left(\frac{c}{d}\right) = \frac{ab_1\alpha}{dd_1\beta}, \quad \left(\frac{a'}{b'}\right)\left(\frac{c'}{d'}\right) = \frac{a'b_1'\alpha}{d'd_1'\beta}$$

当 $c = 0$ 时, 我们定义

$$\left(\frac{a}{b}\right)\left(\frac{0}{d}\right) = \left(\frac{0}{d}\right).$$

集合 K 经过这样定义加法和乘法之后成为一体, 称为 R 的商体. 今往证明其适合体之诸条件:

I. 对加法运算成一 Abel 群. 易见 $\frac{0}{d}$ 相当于 0 元素, 而 $-\frac{a}{b}$ 相当于 $\frac{a}{b}$ 的逆元素. 证明甚易, 读者自证之.

II. 非零元素对乘法成一群. 这一证明也略去. 其中 $\frac{d}{d}$ 相当于么元素, 而 $\frac{b}{a}$ 相当于 $\frac{a}{b}$ 的逆元素.

III. 分配律成立. 首先我们来证明左分配律:

$$\left(\frac{a}{b}\right)\left(\frac{c}{d} + \frac{e}{f}\right) = \left(\frac{a}{b}\right)\left(\frac{c}{d}\right) + \left(\frac{a}{b}\right)\left(\frac{e}{f}\right).$$

设 $bb_1 = cc_1, dc_1d_1 = fc_1f_1 = m$, 即

$$\begin{aligned}\left(\frac{a}{b}\right)\left(\frac{c}{d} + \frac{e}{f}\right) &= \left(\frac{ab_1d_1}{bb_1d_1}\right)\left(\frac{cc_1d_1 + ec_1f_1}{m}\right) \\ &= \left(\frac{ab_1d_1}{bb_1d_1}\right)\left(\frac{bb_1d_1}{m} + \frac{ec_1f_1}{m}\right),\end{aligned}$$

故在证明中不妨假定 $d = f, c = b$, 即只需证明

$$\left(\frac{a}{b}\right)\left(\frac{b+e}{d}\right) = \frac{a}{d} + \left(\frac{a}{b}\right)\left(\frac{e}{d}\right)$$

即足.

设 $n = bb_1 = ee_1$, 此式的右边等于

$$\frac{a}{d} + \frac{ab_1}{de_1} = \frac{ae_1 + ab_1}{de_1},$$

而左边等于

$$\left(\frac{a}{b}\right)\left(\frac{(b+e)e_1}{de_1}\right)=\left(\frac{a}{b}\right)\left(\frac{b(e_1+b_1)}{de_1}\right),$$

于是左右两边完全符合.

右分配律的证明比较容易. 由于在证明

$$\left(\frac{a}{b}+\frac{c}{d}\right)\left(\frac{e}{f}\right)=\left(\frac{a}{b}\right)\left(\frac{e}{f}\right)+\left(\frac{c}{d}\right)\left(\frac{e}{f}\right)$$

时, 不妨假定 $b=d=e$.

如果写 $\frac{ac}{c}=a, \frac{c}{bc}=b^{-1}$, 则 $\frac{a}{b}=ab^{-1}$. 如欲 $(ab^{-1})(cd^{-1})=ef^{-1}$, 一个自然条件是存在两元素 b_1, c_1, 使 $b^{-1}c=b_1c_1^{-1}$, 即 $bb_1=cc_1$, 也即 b, c 有右公倍数. 由此可见, 从环建体, 有右公倍数这一条件是自然的.

在 $\frac{ac}{c}=a$ 的了解下, 体 K 包有 R 作为其自己的子环, 而在 $\frac{c}{bc}=b^{-1}$ 的了解下, 体 K 是包有 R 的最小体.

在交换环中, 任二元素显然有公倍数, 故在无零因子的情况下, 就可以利用上述的理论, 从环来建体. 最具体的例子是: 从整数环到有理数域, 从多项式环到有理函数域, 从整函数环到半纯函数域等等. 但是除了交换环是有右公倍数的环以外, 是否还存在着有右公倍数的非交换环, 下一节我们将回答这个问题.

§3 多项式环

命 K 为一体. 形如

$$f(x)=\sum_{i=0}^{m}a_ix^i \quad (a_0, a_1, \cdots, a_n \in K)$$

的式子称为不定子 x 的多项式. 若 $a_n \neq 0$, 则 n 称为这多项式的次数, 记作 $\partial^0 f$.

设

$$g(x)=\sum_{i=0}^{m}b_ix^i.$$

我们可以定义两多项式的加和乘:

$$f(x)+g(x)=\sum_i(a_i+b_i)x^i,$$
$$f(x)g(x)=\sum_{i,j}a_ib_jx^{i+j}.$$

由定义立刻看出

$$\partial^0(f+g) \leqslant \max(\partial^0 f, \partial^0 g),$$
$$\partial^0(fg) = \partial^0 f + \partial^0 g.$$

所有 x 的多项式成一环, 我们用 $K[x]$ 表示此环. 称为由体 K 导入不定子 x 所得出的多项式环. 环 $K[x]$ 的中心就是由 K 的中心 Z 所得出的环 $Z[x]$.

极易证明 $K[x]$ 是无零因子的. 我们现在再证明其中任二元素都有右公倍式. 换言之, 对任二多项式 $f(x)$ 及 $g(x)$, 常有二多项式 $f_1(x)$ 及 $g_1(x)$(非零的), 使

$$f(x)g_1(x) = g(x)f_1(x).$$

我们在 $\partial^0 f+\partial^0 g$ 上行归纳法. 当 $\partial^0 f+\partial^0 g=0$ 时此结论显然正确. 设 $\partial^0 f+\partial^0 g>0$ 而 $\partial^0 f \geqslant \partial^0 g$, 则 $f(x)-g(x)b_m^{-1}a_n x^{n-m}$ 的次数与 $g(x)$ 的次数和低于 $\partial^0 f+\partial^0 g$. 故有二多项式 $f_2(x)$ 及 $g_2(x)$ 使

$$(f(x)-g(x)b_m^{-1}a_n x^{n-m})g_2(x) = g(x)f_2(x),$$

故得

$$f(x)g_2(x) = g(x)(f_2(x)+b_m^{-1}a_n x^{n-m}g_2(x)).$$

若 $\partial f^0 < \partial^0 g$, 可同法证之.

有此二性质, 我们可以从多项式环 $K[x]$ 上建立一个体来. 这个体中元素的形式是

$$f(x)(g(x))^{-1},$$

此处 $f(x)$ 及 $g(x)$ 都是 $K[x]$ 中的元素. 所得的体称为 K 上的不定子 x 的有理函数体, 用 $K(x)$ 来表它. $K(x)$ 以 K 为其子体, 而 $K(x)$ 称为体 K 的单超越扩体.

定理 1　命 Z 表 K 的中心, 则 $Z(x)$ 是 $K(x)$ 的中心.

【证】　先述若干十分明显的事实: 1) 若 $\dfrac{f(x)}{g(x)}$ 在 $K(x)$ 的中心中, 则 $\dfrac{g(x)}{f(x)}$ 亦然, 并且其逆亦真; 2) 若 $\dfrac{f(x)}{g(x)}$ 在 $K(x)$ 的中心中, 则 $\dfrac{f(x)x}{g(x)}$ 亦然, 并且其逆亦真.

假定 $\dfrac{f(x)}{g(x)}$ 在 $K(x)$ 的中心中, 我们将在 $\partial^0 f+\partial^0 g$ 上施归纳法. 当 $\partial^0 f+\partial^0 g=0$ 时, 此定理显然. 若 $f(0)=0$ 或 $g(0)=0$ 时, 由 2)及归纳法假定也知此定理真实.

今假定 $g(0)\neq 0, f(0)\neq 0$, 并可假定 $\partial^0 g \leqslant \partial^0 f$(由 1)) 及 $g(0)=1$. 由于 $\dfrac{f(0)}{g(0)}$ 在中心中, 故 $f(0)$ 在中心中. 故

$$\frac{f(x)}{g(x)} - f(0)$$

也在 $K(x)$ 的中心中. 因而

$$\frac{f_1(x)}{g(x)}, \quad f_1(x) = \frac{f(x) - f(0)g(x)}{x}$$

也在 $K(x)$ 的中心中. 由于 $\partial^0 f_1 + \partial^0 g < \partial^0 f + \partial^0 g$, 故由归纳法假定知 $\frac{f_1(x)}{g(x)}$ 属于 $Z(x)$. 因此 $\frac{f(x)}{g(x)}$ 属于 $Z(x)$. 定理于是证明.

我们也可以把 §1 例 7 作进一步推广:

设 K 为体, Z 为 K 的中心. 命 $f(x)$ 为 $Z[x]$ 中的一元, 并且在 $K[x]$ 中不可分解. 则以 $f(x)$ 为模, 将 $K[x]$ 中的多项式分类, 这些类成一体.

又假定 α 是适合于 $f(x)=0$ 的元素, 且 α 与 K 内的元素可交换, 则形如

$$a_0 + a_1\alpha + \cdots + a_{n-1}\alpha^{n-1} \quad (a_0, \cdots, a_{n-1} \in K)$$

的元素成一体, 此处 $n = \partial^0 f$. 这样与以上所得到的体本质上相同. 这体称为 K 的单代数扩体, 以 $K(\alpha)$ 代表它.

§4 同　态

命 R 与 R' 为二环, 对 R 中的任一元素 a, R' 中有一元素 a' 与之对应, 且当 a 经过 R 的所有元素时, a' 也经过 R' 的所有元素. 如果这种对应更适合以下的关系:

(1) $$(a+b)' = a' + b',$$

及

(2) $$(ab)' = a'b',$$

则称此二环的对应为同态; 如果把条件 (2) 换为

(2′) $$(ab)' = b'a',$$

则此项对应关系称为反同态; 又如果将条件 (2) 换为

(3) $$(a^2)' = a'^2,$$

及

(4) $$(aba)' = a'b'a',$$

则此关系称为半同态.

若对应是一对一的, 则此同态, 反同态和半同态各称为同构, 反同构和半同构.

同态, 反同态都是半同态, 但其逆如何?

定理 1 设 R 与 R' 为二环, R' 无零因子, 若 R 与 R' 间有半同态对应, 则此对应必为同态或反同态.

【证】 由 (1) 及 (4) 得

$$\begin{aligned}(abc+cba)' &= ((a+c)b(a+c)-aba-cbc)' \\ &= (a'+c')b'(a'+c')-a'b'a'-c'b'c' \\ &= a'b'c'+c'b'a'.\end{aligned}$$

再由 (3) 及 (4) 得出

$$\begin{aligned}&((ab)'-a'b')((ab)'-b'a') \\ &\quad = ((ab)')^2+a'(b')^2a'-(a'b'(ab)'+(ab)'b'a') \\ &\quad = ((ab)^2)'+(ab^2a)'-(ab(ab)+(ab)ba)' \\ &\quad = 0.\end{aligned}$$

因 R' 中无零因子, 故

$$(ab)'=a'b' \quad 或 \quad b'a'.$$

若 R' 为交换环, 则定理 1 成立. 若 R' 非交换环, 且对此半同态, 有二元 a 与 b, 使

(5) $$(ab)'=a'b'\neq b'a'.$$

今利用"传染法"来证明对于 R 中任一 e 常有

(6) $$(eb)'=e'b', \quad (ae)'=a'e'.$$

事实上, 若 $(eb)'=b'e'\neq e'b'$, 则

$$a'b'+b'e'=((a+e)b)'=\begin{cases}(a'+e')b' \\ 或 \\ b'(a'+e').\end{cases}$$

这和所设相违背. 类似地可证 $(ae)'=a'e'$.

今假定有二元素 c 与 d, 使

(5) $$(cd)'=d'c'\neq c'd'.$$

与前面一样, 对 R 中任一元 e 常用

$$(ed)' = d'e', \quad (ce') = e'c'. \tag{6'}$$

考查下面的式子:

$$((a+c)(b+d))' = \begin{cases} (a'+c')(b'+d') \\ \text{或} \\ (b'+d')(a'+c') \end{cases}$$

由等式 (5), (6), (5′) 及 (6′) 可知, 以上两种情况都是不可能的, 故知对于任意一对 c 与 d, 常有 $(cd)' = c'd'$. 故为同态.

同样可以得反同态的情况. 定理于是获证.

特别是体与体之间的半同构一定是同构或反同构.

R 与 R' 之间之对应关系如满足以下二条件者称为 Jordan 同态:

$$(a+b)' = a' + b' \tag{1}$$

及

$$(ab+ba)' = a'b' + b'a'. \tag{2''}$$

定理 2 凡半同态一定是 Jordan 同态.

【证】

$$\begin{aligned}(ab+ba)' &= ((a+b)^2 - a^2 - b^2)' \\ &= (a'+b')^2 - a'^2 - b'^2 = a'b' + b'a'.\end{aligned}$$

定理 3 若环 R' 中有次之性质: 由 $2a = 0$ 可以得出 $a = 0$, 则 Jordan 同态一定是半同态.

【证】 由 (1) 及 (2″) 各得

$$(a^2+a^2)' = 2(a^2)',$$
$$(a^2+a^2)' = 2(a')^2,$$

故得 $(a^2)' = a'^2$. 又由

$$2aba = a(ba+ab) + (ba+ab)a - (a^2b + ba^2)$$

可得

$$(aba)' = a'b'a'.$$

定理 4　二体 K 与 K' 间的同态 (或反同态) 必为同构 (或反同构).

【证】 命 $a \to a'$ 为 K 与 K' 间的同态, 以 N 表 K 中所有的对应于 K' 中 0 的元素所成的集合. 若能证明 N 只有零元素, 则此对应是一意的. 盖若 $a \to a', b \to a'$, 则 $(a-b) \to 0$. 故得 $a = b$.

若 N 中有一元素 $c \neq 0$, 命 b 为 K 中的任一元素, 则

$$b = (bc^{-1})c \to (bc^{-1})'c' = 0,$$

即 K 中所有的元素皆对应于 K' 中的零元素. 这与 K' 为体的假设相违背.

此定理对半同态也真.

一体与其自己的同构对应称为该体的自同构 (同样定义反自同构, 半自同构等等). 连续运用两次自同构还是一个自同构. 一体的诸自同构对于自同构的连续运用这种运算而言组成一群, 其单位元称为全等自同构 (或单位自同构). 连续运用两次反自同构, 便成为一个自同构. 如果 K 是体而非域, 它有一个反自同构, 则诸自同构与反自同构成一群, 它以所有自同构所成的群为正规子群, 其指数为 2.

体之半自同构的研究与一维射影几何有本质上的关系. 因之, 本章中将列举一些常见的域和体的半自同构.

§5　素域与实数域的自同构

一素域显然只存在一个自同构 $a \leftrightarrow a$, 即使每一元素都不变的自同构. 盖 $0 \leftrightarrow 0, 1 \leftrightarrow 1$, 故自然数 $m \leftrightarrow m$. 若特征为 p, 结论显然正确. 若特征为零, 则 $\frac{m}{n} \leftrightarrow \frac{m}{n}$, 即任一有理数都不变, 故得所云.

最常见的域是实数域, 但定出实数域的自同构并不是一个容易问题. 同时, 解决了这一个问题, 也就解决了直线上射影几何的基本定理. 在数学史中有过多次不成功的尝试, 到 1880 年 Dardoux 才首先解决了这一问题.

定理 1　实数域仅有全等自同构.

【证】 今用 $R^{\#}$ 表示所有实数组成的域, 假定

$$a \to a'$$

是 $R^{\#}$ 的一个自同构. 由 $1 \leftrightarrow 1$ 可知所有的整数都对应于自己. 因之, 每一个有理数也对应于自己.

因为 $R^{\#}$ 中任一正数都可以表成为其中一数的平方, 其逆也真. 由 $a^2 \to a'^2$ 可知, 正数一定对应于正数. 因此, 如果 $a > b$, 则 $a' > b'$, 并且反之亦然.

命 γ 是一实数, 则我们可以找出两个有理数所成的序列:

$$a_1 \leqslant a_2 \leqslant \cdots \leqslant \gamma,$$
$$b_1 \geqslant b_2 \geqslant \cdots \geqslant \gamma,$$

并且 $\lim\limits_{n\to\infty} a_n = \lim\limits_{n\to\infty} b_n = \gamma$. 设 $\gamma \to \gamma'$. 因为 $a_i' = a_i, b_i' = b_i$, 所以

$$a_1 \leqslant a_2 \leqslant a_3 \leqslant \cdots \leqslant \gamma',$$
$$b_1 \geqslant b_2 \geqslant \cdots \geqslant \gamma',$$

故得 $\gamma = \gamma'$. 即明所证.

注意, 有理数所成的域 R 仅有一个自同构, 实数域 $R^{\#}$ 也只有一个自同构, 但是在 R 与 $R^{\#}$ 间的域确可以有其他的自同构. 例如, 由 $a + b\sqrt{2}, (a, b \in R)$ 所成的域, 就有两个自同构:

$$a + b\sqrt{2} \leftrightarrow a + b\sqrt{2}$$

及

$$a + b\sqrt{2} \leftrightarrow a - b\sqrt{2}.$$

又如在有理数添进 π(圆周率) 所得的域有以下一些自同构:

$$\pi \leftrightarrow \frac{a\pi + b}{c\pi + d},$$

此处 a, b, c, d 是有理数, 且 $ad - bc \neq 0$. 所以这域有无穷个自同构. (这域也就是有理系数的 π 的有理函数所成的域.)

现在要问复数域的自同构是怎样的? 以前数学家曾猜测过复数域 C 上只有两个自同构, 即

(1) $$a + bi \leftrightarrow a + bi \quad (\text{全等})$$

及

(2) $$a + bi \leftrightarrow a - bi \quad (\text{共轭}).$$

根据 1910 年 Steinitz 发表的关于域的代数理论, 这个猜测并不正确, 我们将在 §7 中谈到. 但是在此我们将指出, 在某些条件下, 这猜测是正确的.

定理 2 命 F 为所有有理复虚数所成的域, 即当 a, b 为有理数, $a + bi$ 所成的域. 此域仅有两个自同构: 全等与共轭.

【证】 有理数显然变为其自己. 假定 $i \to j$, 则由 $i^2 = -1$ 可知 $j^2 = -1$, 故 $j = i$ 或 $-i$. 这就证明了定理.

定理 3　域 C 的连续性的自同构仅有两个: 全等与共轭.

此由定理 2 及 F 在 C 中处处稠密的性质推出.

所可注意者, 在实数域中连续性乃自同构的推论, 而复数域中不能推出自同构的连续性.

定理 4　域 C 中变实数为实数的自同构也仅有二个: 全等与共轭.

【证】 此时由 C 的自同构可以导出 $R^{\#}$ 的自同构. 由定理 1, 此自同构变任一实数为其自己, 由此及定理 2 之证明即得出本定理.

§6　线性相关与有限域

定义 1　命 K 为一体, L 为其一子体, 若对 K 中之 n(有限) 个元素 $t_1, \cdots, t_n$, 在 L 中有不全为零之 $a_1, \cdots, a_n$, 使

$$a_1t_1 + a_2t_2 + \cdots + a_nt_n = 0,$$

则 $t_1, \cdots, t_n$ 称为对 L 左线性相关 (或互依). 若无此 a_i 存在, 则称为左线性无关.

若 K 之一子集 S 中任意有限个元素皆对 L 左线性无关, 则此集 S 被称为对 L 左线性无关.

定理 1　若 L 是 K 的子体, 则在 K 中有一对 L 最大的左线性无关集存在. 换言之, K 中有一集 S, 其中任意有限个元素皆对 L 左线性无关, 但若再加入 K 中任一元素, 即丧失此种性质.

【证】 假定 K 中的非零元素已经排成良序: $\{e_\omega\}$, 我们现在定义一串的左线性无关集 $\{S_\omega\}$: 若 $\omega' < \omega$, 则 $S_{\omega'} \subseteq S_\omega$. 今用超限归纳法定义这些 S_ω 如下:

首集就是 $S_1 = \{e_1\}(e_1 \neq 0)$. 若对 $\nu < \omega$ 之 S_ν 皆已定义, 今定义 S_ω, 若 e_ω 与 $\bigcup\limits_{\nu<\omega} S_\nu$ *) 线性相关, 即命 $S_\omega = \bigcup\limits_{\nu<\omega} S_\nu$; 若 e_ω 与 $\bigcup\limits_{\nu<\omega} S_\nu$ 线性无关, 则命 S_ω 为集合 $\bigcup\limits_{\nu<\omega} S_\nu$ 再添上 e_ω所成的集合

显然 S_ω 是线性无关的, 且当 $\nu < \omega$ 时, $S_\nu \subseteq S_\omega$. 于是所有的 S_ω 的总集就是所求的最大的左线性无关组.

定义 2　K 对 L 的最大左线性无关集 (为简便起见) 称为 K 对 L 的左线性基.

若不致于引起误解, 我们将简称为线性基或迳称为基.

显然有

---

*) $\bigcup\limits_{\nu<\omega} S_\nu$ 表示所有 $\nu < \omega$ 的集合 S_ν 的元素的总集合.

定理 2 设 L 是 K 的子体, 一元素组 S 是线性基的充分且必要条件, 为 K 中元素可以唯一地表为 S 中有限个元素的一次式:

$$\sum_{i=1}^{n} a_i x_i \quad (a_i \in L, x_i \in S).$$

定理 3 设 L 是 K 的子体, 且有一个有限基 $B = \{e_1, \cdots, e_n\}$, 则其他的基 B' 也是恰有 n 个元素.

【证】 命 B' 表另一基 $\{e'_\omega\}$, 假定 B' 的元素的个数多于 n, 由于 B 是基, 所以 $\{e'_1, e_1, \cdots, e_n\}$ 是线性相关的. 吾人顺次考查 $\{e'_1, e_1, \cdots, e_n\}$ 丢掉那些元素是与它前面的元素线性相关的, 如此得出一个基 $\{e'_1, f_2, \cdots, f_{n'}\}$, 此处 $f_2, \cdots, f_{n'}$ 是 $e_1, \cdots, e_n$ 中的 $n'-1$ 个元素, 而 $n'+1 \leqslant n$.

再考查 $\{e'_2, e'_1, f_2, \cdots, f_{n'}\}$, 由于 e'_2, e'_1 是线性无关的, 自 f_2 起, 逐一研究, 丢掉那些与它前面的元素线性相关的, 因而得出

$$\{e'_2, e'_1, g_3, \cdots, g_{n''}\} \quad (n''+2 \leqslant n).$$

此处 $g_3, \cdots, g_{n''}$ 是 $f_2, \cdots, f_{n'}$ 中的元素, 也是 $e_1, \cdots, e_n$ 中的元素, 续行此法, 经过有限步之后, 得一组基 $\{e'_m, \cdots, e'_1\}$ $(m \leqslant n)$, 这和 B' 的元素的个数多于 n 相矛盾.

若 B 的元素的个数少于 B' 的元素的个数, 可以得出同样的矛盾. 故 B 的元素的个数与 B' 的元素的个数相等. 故得定理.

由此定理可见, 基的元素的个数, 并不因基的选择而变, 这个个数称为体 K 对 L 的次数, 用 $[K:L]$ 来表示. 若 K 对 L 的基有无限多个元素, 则记为

$$[K:L] = \infty.$$

定理 4 若 L 是 K 的子体, M 是 L 的子体, 则

$$[K:M] = [K:L][L:M].$$

【证】 如果其中有一个是 ∞, 则定理显然, 自毋待证.

假定 $s_1, \cdots, s_m$ 是 K 对 L 的基, $e_1, \cdots, e_n$ 为 L 对 M 的基, 我们要证明 $e_j s_k (1 \leqslant k \leqslant m, 1 \leqslant j \leqslant n)$ 就是 K 对 M 的基. 由假定, K 中任一元素 a 可以表为

$$\sum_{k=1}^{m} a_k s_k \quad (a_k \in L).$$

因为 $a_k \in L$, 故 a_k 又可以写成为

$$\sum_{j=1}^{n} a_{kj} e_j \quad (a_{kj} \in M).$$

故得

$$a=\sum_{k=1}^{m}\sum_{j=1}^{n}a_{kj}e_js_k,$$

即 K 中任一元素可以表成为 e_js_k 的一次式.

今再证明 $\{e_js_k\}$ 是线性无关的. 盖如 M 中有 a_{kj} 使

$$\sum_{k=1}^{m}\sum_{j=1}^{n}a_{kj}e_js_k=0,$$

则由 $s_1,\cdots,s_m$ 的无关性, 可知

$$\sum_{j=1}^{n}a_{kj}e_j=0.$$

又因 $\{e_j\}$ 线性无关, 故必有 $a_{kj}=0$. 于是证明了定理.

〔**例 1**〕 四元数体 Q 对其中心的次数为 4. 四元数体对 $\{1,i\}$ 所演成的子体的次数是 2.

关于 §3 中所谈到的单代数扩体, 有次之

定理 5 $[K(\alpha){:}K]=n$.

定理 6 (Wedderburn) 仅有有限个元素组成的体 K 一定是域, 其元素的个数为其特征数 p 的乘幂.

【**证**】 我们采用 Witt 的证明. 命 P 为 K 的素体. $[K{:}P]=m$, 由上所述可见 K 的元素的个数等于 p^m.

设 K 的中心 Z 有 q 个元素及 $[K{:}Z]=n$, 则 K 显然有 q^n 个元素. 命 a 为 K 中之任一元素, 与 a 可交换的元素所成的集合以 K_a 记之. K_a 为一体, 且包有 Z, 故 K_a 的元素个数为 q^d. 因 K_a 是 K 的子体, 由定理 4, d 为 n 的因子. 因 K_a 中零以外的元素成为 K 的乘法群的一子群, 故 K 中与 a 共轭的元素的个数为 $\dfrac{q^n-1}{q^d-1}$. 事实上, 若以 K^* 及 K_a^* 分别表示 K 及 K_a 的乘法群, 将 K^* 对于子群 K_a^* 分成陪集, 如此一共得到 $\dfrac{q^n-1}{q^d-1}$ 个陪集, 而且同一陪集的元素把 a 变为同一元素, 不同陪集的元素把 a 变为不同元素. 命 $b\in K^*,k\in K_a^*$, 可知

$$bka(bk)^{-1}=bab^{-1}.$$

又由

$$b_1ab_1^{-1}=b_2ab_2^{-1},\quad b_2^{-1}b_1a=ab_2^{-1}b_1$$

可知 $b_2^{-1}b_1=k\in K_a^*$. 故与 a 共轭的元素的个数等于 K^* 对于子群 K_a^* 的陪集的个数 (或称指数).

现在把 K 的乘法群分为共轭元素组, 因而得出等式

$$q^n - 1 = q - 1 + \sum_{d|n}{}' \frac{q^n - 1}{q^d - 1}, \tag{1}$$

此处 $\sum\limits_{d|n}{}'$ 中的 d 是经过某些 n 的因子, 并不一定经过 n 的所有因子.

设 $\varphi(n)$ 为 $1, 2, \cdots, n$ 中与 n 互素的整数的个数. 命

$$\Phi_n(x) = \prod (x - \xi_i),$$

此处 ξ_i 经过所有的 n 次单位原根, 则 $\Phi_n(x)$ 是一个 $\varphi(n)$ 次带整数系数的多项式, 且对任一 $d|n(0 < d < n)$, 常有

$$\Phi_n(x) \Big| \frac{x^n - 1}{x^d - 1}.$$

命 $x = q$, 可知

$$\Phi_n(q) \Big| \frac{q^n - 1}{q^d - 1}.$$

由 (1) 可知

$$\Phi_n(q) | (q - 1).$$

若 $n > 1$, 则

$$|\Phi_n(q)| = \prod |q - \xi_i| > (q - 1)^{\varphi(n)} \geqslant q - 1.$$

与 $\Phi_n(q)|(q-1)$ 相违背. 故 $n = 1$, 即 $Z = K$.

定义 3 有限个元素所成的域谓之有限域.

定理 7 有限域的乘法群是一循环群.

此定理乃下述群论中的定理的一个推论.

定理 8 设 G 为一有限群, 其阶为 N. 若对每一自然数 n, 在 G 中至多有 n 个元素适合于 $x^n = 1$, 则 G 为一循环群.

【证】 若 a 是一 d 阶的元素, 则 $d|N$, 且 $1, a, \cdots, a^{d-1}$ 是适合于

$$x^d = 1 \tag{2}$$

的元素. 由假定, 此为 (2) 式的一切解, 故有 $\varphi(d)$ 个元素, 其阶是 d. 因 G 之任一元素的阶必为 N 的因子, 故得

$$N = \sum_{d}{}' \varphi(d), \tag{3}$$

此处 d 过 N 的某些因子.

另一方面, $1,\cdots,N$ 中与 N 的最大公约数等于 δ 者的个数显然等于 $\varphi\left(\frac{N}{\delta}\right)$, 故

$$N=\sum_{\delta\mid N}\varphi\left(\frac{N}{\delta}\right)=\sum_{d'\mid N}\varphi(d'),$$

此处 d' 过 N 的一切因子. 故可见 (3) 中之 d 亦当过 N 的一切因子, 即必有一个元素其阶为 N. 即得定理.

因在域中, $x^n=1$ 的根的个数不超过 n, 故定理 7 获证.

定理 9　具有 p^n 个元素之有限域, 恰有 n 个自同构:

$$a\to a^{p^i}\quad(i=0,1,\cdots,n-1),\tag{4}$$

故自同构也成一 n 阶的循环群.

【证】　先证明 $a\to a^p$ 是一自同构. 若 $a\to a^p,b\to b^p$, 而 $a^p=b^p$, 则 $(a-b)^p=0$, 故 $a=b$. 故对应是一意的. 由

$$(a+b)^p=a^p+b^p,\quad(ab)^p=a^pb^p,$$

可知 $a\to a^p$ 是一自同构. 因之, (4) 表示 n 个自同构.

今再证明这 n 个自同构外, 无其他的自同构. 域 K 的乘法群既然是循环群 (定理 7), 命 a 为这群的演出元素, 即 K 内的非零元素可以表为

$$a^i\quad(i=0,1,2,\cdots,p^n-1).$$

多项式

$$f(x)=\prod_{i=0}^{n-1}(x-a^{p^i})$$

的系数是 $a,a^p,\cdots,a^{p^{n-1}}$ 的初等对称函数. 设其一为

$$g(a,a^p,\cdots,a^{p^{n-1}})$$

则

$$\begin{aligned}(g)^p&=g(a^p,a^{p^2},\cdots,a^{p^{n-1}},a)\\&=g(a,a^p,\cdots,a^{p^{n-1}}),\end{aligned}$$

即 g 的 p 次幂仍为其自己. 但 $x^p=x$ 仅有 p 个根 $0,1,\cdots,p-1$, 故 g 在素域中. 因此 $f(x)$ 的系数也都在素域中. 故任一自同构使 $f(x)$ 不变. 由此立得 a 一定变为 $a,a^p,\cdots,a^{p^{n-1}}$ 之一. 定理已经证明.

§7 代数相关与复数域的自同构

本节中假定 E 是一域, F 是它的子域.

定义 1 若 E 中的 n 个元素 $x_1, \cdots, x_n$ 对 F 有一代数关系, 则这 n 个元素名为对 F 代数相关; 所谓代数关系, 乃指存在一个系数在 F 中的多项式 $f(X_1, \cdots, X_n)$, 使得

$$f(x_1, \cdots, x_n) = 0.$$

定义 2 若一组元素 S 中, 任意有限个元素对 F 皆无代数关系, 则此 S 称为对 F 代数无关.

定义 3 若一元素 x 满足系数属于 F 的方程式, 则称此 x 对 F 是代数的. 否则称为超越的.

与线性相关性相似, 我们有以下的代数相关性定理, 因其证明与前者完全相同, 故从略.

定理 1 E 中有一最大的对 F 代数无关组存在.

定义 4 此最大的对 F 代数无关组称为 E 对 F 的超越基.

定理 2 若 S 是 E 对 F 的一组代数无关的元素, 则 S 是 E 对 F 的超越基的充分且必要条件为 E 内任一元素对 $F(S)$ 是代数的, 此处 $F(S)$ 代表最小的域, 既包 F, 又包 S 的.

定理 3 设 E 对 F 有一组有限个元素的超越基 $B = \{x_1, \cdots, x_n\}$, 则任一超越基也恰有 n 个元素.

此数 n 定义为 E 对 F 的维数, 以 $\left(\frac{E}{F}\right)$ 记之.

若超越基的元素个数无限, 则记为 $\left(\frac{E}{F}\right) = \infty$.

若 E 是 F 的代数扩域, 换言之, E 中的元素对 F 都是代数的, 则 $\left(\frac{E}{F}\right) = 0$. 若 $F(x_1, x_2, \cdots, x_n)$ 表示系数在 F 中的 n 个未定元的一切有理函数所成的域, 则 $\left(\frac{F(x_1, \cdots, x_n)}{F}\right) = n$.

定义 5 设 F 是一域, 若系数在 F 中的多项式在 F 中皆可分解为一次式之积, 即称 F 为代数封闭域.

复数域是一个代数封闭域, 因此以下所讨论的定理对复数域也适用, 并可由此看出复数域自同构的结构.

定理 4 设 E 是一个代数封闭域, F 为其子域, 则 E 中有一对 F 代数无关组 $T = \{t_\omega\}$, 使 E 对 $F(T)$ 是代数的. 又由 T 中诸元素之任一置换, 可以得出 $F(T)$ 的自同构, 并且这些自同构使 F 中的元素不变.

【证】 T 之存在可由定理 1 及 2 得出.

设 π 是 T 的一个置换, 因 $F(T)$ 中的每一元素 t 皆可表成为系数在 F 中 T 内 $t_{\alpha_1},\cdots,t_{\alpha_n}$ 的有理函数, 故可命

$$t=H(t_{\alpha_1},\cdots,t_{\alpha_n}).$$

今定义对应 f 为

$$f(t)=H(\pi(t_{\alpha_1}),\cdots,\pi(t_{\alpha_n})).$$

如此之 f 即为 $F(T)$ 对其自己的一一对应. 盖若 f 将 $F(T)$ 中的不同的元素 H_1 及 H_2 变为 $F(T)$ 中的同一元素, 即

$$H_1(\pi(t_{\alpha_1}),\cdots,\pi(t_{\alpha_n}))=H_2(\pi(t'_{\alpha_1}),\cdots,\pi(t'_{\alpha_n})),$$

则 $\pi(t_{\alpha_1}),\cdots,\pi(t_{\alpha_n}),\pi(t'_{\alpha_1}),\cdots,\pi(t'_{\alpha_n})$ 之间有一代数关系, 此为不可能.

此项对应使 $F(T)$ 的每一元素皆被对应到. 盖若

$$s=H(t_{\alpha_1},\cdots,t_{\alpha_n}),$$

则

$$s=f(H(\pi^{-1}(t_{\alpha_1}),\cdots,\pi^{-1}(t_{\alpha_n}))).$$

最后显然有

$$f(s+t)=f(s)+f(t),\ f(st)=f(s)f(t),$$

故 f 是一个使 F 不变的, $F(T)$ 的自同构.

定理 5　设 F 有一自同构 $a\leftrightarrow a^{\tau}$. 命

$$p(x)=a_nx^n+a_{n-1}x^{n-1}+\cdots+a_0$$

是 $F[x]$ 中的一个不可分解的多项式, 在 E 中有一根 α. 若

$$p^{\tau}(x)=a_n^{\tau}x^n+a_{n-1}^{\tau}x^{n-1}+\cdots+a_0^{\tau}$$

在 E 中有一根 β, 则 $F(\alpha)$ 与 $F(\beta)$ 同构.

【证】 此 $p^{\tau}(x)$ 也不可分解. 盖若不然, 我们可以施行 τ 之逆置换而得出一矛盾.

$F(\alpha)$ 与 $F(\beta)$ 的对应确定为

$$q_0+q_1\alpha+\cdots+q_{n-1}\alpha^{n-1}\leftrightarrow q_0^{\tau}+q_1^{\tau}\beta+\cdots+q_{n-1}^{\tau}\beta^{n-1}.$$

这一对应极易证明是一同构.

显然有

定理 6 若一单扩域 $F(\alpha)$ 有一自同构, 使 F 中的元素不变, 此自同构使 α 对应于 β, 则 α 与 β 适合同一不可分解多项式.

因此, 如果 $p(x)=0$ 在 $F(\alpha)$ 中有 r 个根, $\alpha=\alpha_1,\cdots,\alpha_r$, 则在 $F(\alpha)$ 中恰有 r 个自同构, 由 $\alpha\leftrightarrow\alpha_i$ 且使 F 的元素保持不变.

例如, 设 F 是有理数域 R, 则 $F(\sqrt[3]{2})$ 仅有一个自同构, 但若 F 是域 $R(e^{2\pi i/3})$, 则 $F(\sqrt[3]{2})$ 有三个自同构:

$$\sqrt[3]{2}\leftrightarrow\sqrt[3]{2},\quad \sqrt[3]{2}\leftrightarrow\sqrt[3]{2}e^{2\pi i/3},\quad \sqrt[3]{2}\leftrightarrow\sqrt[3]{2}e^{4\pi i/3}.$$

定理 7 设 E 对 F 是代数的, 又 E 是代数封闭的, 如果有一个同构对应把 E 映入自己, 且引出 F 的一个自同构, 则此同构关系就是 E 的自同构.

【证】 设所说的同构关系是 $\alpha\leftrightarrow\sigma(a)$, 假定 $\sigma(E)=E^*$. 如果 $E^*=E$, 则定理毋须证明. 如 $E^*\neq E$, 则 E 中至少有一元素 a 不在 E^* 中, 假定 a 所适合的 F 上不可分解方程是

$$f(x)=0,$$

此方程有一根 a 在 E^* 之外. 运用 σ 之逆, 命对应于 $f(x)$ 的多项式是 $g(x)$, 则 E 中不能有 $g(x)=0$ 的一切根, 此为不可能者 (注意 f 与 g 的次数相同).

定理 8 (Steinitz) 设 E 对 F 是代数的, 又 E 为代数封闭, 则 F 的任一自同构可扩张为 E 的自同构. 换言之, 如果 $a\leftrightarrow f(a)$ 是 F 的一自同构, 则可找到 E 的一个自同构 $a\leftrightarrow e(a)$, 使在 F 上 $f(a)=e(a)$.

【证】 把 E 中不在 F 上的元素排成良序集

$$e_1<\ \cdots<\ e_\omega<\ \cdots.$$

今用超限归纳法来证明本定理. 我们作出域的集合 $\{F_\omega\}$:

$$F=F_0\subseteq F_1\subseteq\cdots\subseteq F_\omega\subseteq\cdots,$$

具有以下的性质:

I. 对每一域 F_ω, 有一同构 f_ω 把 F_ω 映入 E 中, 而 $f_0=f$;

II. 若 $\mu<\nu$, 则在 F_μ 上 f_ν 与 f_μ 互相一致; 换言之, 若 $a\in F_\mu$, 则 $f_\nu(a)=f_\mu(a)$.

命 $K=\bigcup\limits_{\nu<\omega}F_\nu$, 此 K 显然是一域. 对 K 我们定义以下的同构 g:

如果 $x\in F_\nu$, 则

$$g(x)=f_\nu(x).$$

g 显然将 K 映入 E 中. 命 $g(K)=K^*$. 定义 $F_\omega=K(e_\omega)$. 设 $p(x)$ 是 e_ω 所满足的系数在 K 中的不可分解多项式, 经同构 g, $p(x)$ 变为 $p^*(x)$, 这 $p^*(x)$ 在 K^* 中也显

然不可分解. 设 e'_ω 是 $p^*(x)=0$ 的根, 且在 E 的排列次序中排在最前的一个 (e'_ω 的存在, 由 E 的代数封闭性可得出). 易见

$$F_\omega = K(e_\omega) \cong K^*(e'_\omega).$$

此项同构关系用 f_ω 来表示. f_ω 在 K 上显然是和 g 一致的. 所以在 $F_\nu(\nu<\omega)$ 上和 f_ν 是一致的.

显而易见, $E=\bigcup\limits_{\omega} F_\omega$. 今定义

$$e(x)=f_\omega(x) \quad (x\in F_\omega),$$

将 f_ω 扩展到 E. e 把 E 映入自己. 由定理 7, e 是 E 的自同构.

§8　超越扩张的自同构

定理 1　设 F 是一域, $F(x)$ 是系数在 F 中的有理函数域 (亦称 F 的单超越扩张), $F(x)$ 的自同构, 其使 F 的元素不变者, 一定是

$$x\to \frac{ax+b}{cx+d} \quad (ad-bc\neq 0).$$

的形式.

【证】　假定该同构把 x 变为 y, 则 $F(x)=F(y)$, 即域 $F(x)$ 也是 y 的有理函数所成的域, 此定理可由下面的定理得出.

定理 2　$F(x)$ 中之任一演出之元素 y 之形式是

$$y=\frac{ax+b}{cx+d} \quad (ad-bc\neq 0).$$

【证】　设

$$y=\frac{f(x)}{g(x)} \quad ((f,g)=1),$$

则 $g(X)y-f(X)$ 是一多项式, 其系数在 $F(y)$ 中. 因 $g(X)\neq 0$, 故可将其写成 $g(X)=g_nX^n+\cdots+g_0\neq 0$, 又 $f(X)=f_mX^m+\cdots$(我们并未假定 $f_m\neq 0$, 故可设 $m>n$). 注意, 如果 $g_ny-f_n=0$, 则 y 在 F 中, 不可能是一演出元素. 故若将 $g(X)y-f(X)$ 写成 X 的多项式, 则其次数 $\geqslant n$. 今先证明此多项式在 $F(y)[X]$ 中不可分解. 盖若在 $F(y)[X]$ 中此式能分解, 则由 Gauss 定理, 此式在 $F[y,X]$ 中可以分解. 因为此式对 y 是一次的, 又 $(f,g)=1$, 故其在 $F[y,X]$ 中不能分解. 因之, $[F(x):F(y)]=\max\{\partial^0 f,\partial^0 g\}$. 但由 $F(x)=F(y)$ 可知 $\partial^0 f\leqslant 1$ 及 $\partial^0 g\leqslant 1$, 即可写 $f(x)=ax+b, g(x)=cx+d$. 因 $y=\dfrac{ax+b}{cx+d}$ 不在 F 中, 故 $ad-bc\neq 0$, 而吾人之定

理即已证明.

定义 设 $f_1,\cdots,f_n$ 是 n 个有理函数, 则变换

$$x_i'=f_i(x_1,\cdots,x_n)\quad(i=1,2,\cdots,n)$$

称为有理变换. 若一有理变换的逆变换也是有理变换, 则此有理变换名为双有理变换.

〔**例 1**〕

$$x'=\frac{x}{x^2+y^2},\quad y'=\frac{-y}{x^2+y^2}.$$

定理 3 设 F 为一域, $F(x_1,\cdots,x_n)$ 是 n 个不定子 $x_1,\cdots,x_n$ 的有理函数所成的域. $F(x_1,\cdots,x_n)$ 的自同构, 其使 F 之每一元素皆不变者, 是下列的形式: 设 $x_1,\cdots,x_n$ 经此自同构变为 $x_1',\cdots,x_n'$, 则 $x_1',\cdots,x_n'$ 与 $x_1,\cdots,x_n$ 间的关系式是一双有理变换.

【证】 因 $F(x_1,\cdots,x_n)=F(x_1',\cdots,x_n')$, 故 x_i' 属于 $F(x_1,\cdots,x_n), x_i$ 属于 $F(x_1',\cdots,x_n')$, 即得

$$x_i'=f_i(x_1,\cdots,x_n)\quad(i=1,\cdots,n);\quad x_i=g_i(x_1',\cdots,x_n')\quad(i=1,\cdots,n),$$

式中 f_i 与 g_i 都是有理函数, 其逆显然成立.

§9 四元数体

命 Q 表实域 F 上的四元数体, 元素 $\bar{a}=a_0-a_1i-a_2j-a_3k$ 称为元素 $a=a_0+a_1i+a_2j+a_3k$ 的共轭元素. $T(a)=a+\bar{a}=2a_0$ 称为元素 a 的迹, $N(a)=a\bar{a}=a_0^2+a_1^2+a_2^2+a_3^2$ 称为元素 a 的范. 显然有

$$T(a+b)=T(a)+T(b),$$
$$N(ab)=N(a)\cdot N(b).$$

易见 $a\to\bar{a}$ 是 Q 的一个反自同构. 因为每一个反自同构都可以从一个自同构乘此反自同构获得, 因此只要求出全部的自同构, 便也知道了全部的反自同构.

对任一四元数 q, 我们可作一自同构

$$a\leftrightarrow qaq^{-1}.$$

这样的自同构称为内自同构.

定理 1 实数域上的四元数体的自同构都是内自同构.

我们现在从更一般的实域上的四元数体 Q 来讨论这个问题.

引理 1　命 a 与 b 为 Q 中二个四元数, 则有一 q 使

$$qaq^{-1} = b \tag{1}$$

的充分且必要的条件是

$$T(a) = T(b), \quad N(a) = N(b).$$

【证】　因为 $q\bar{q} = N(q)$ 在 F 中, 所以由 (1) 显然有

$$\bar{b} = \overline{q^{-1}}\bar{a}\bar{q} = q\bar{a}q^{-1}.$$

即得 $T(a) = T(b)$ 及 $N(a) = N(b)$.

反之, 假定

$$a = a_0 + a_1 i + a_2 j + a_3 k,$$
$$b = b_0 + b_1 i + b_2 j + b_3 k$$

及

$$a_0 = b_0, \quad a_1^2 + a_2^2 + a_3^2 = b_1^2 + b_2^2 + b_3^2.$$

若有一 q 使

$$q(a_1 i + a_2 j + a_3 k)q^{-1} = b_1 i + b_2 j + b_3 k,$$

则 $qaq^{-1} = b$. 故可以假定 $a_0 = b_0 = 0$ 而不失其普遍性.

命

$$q = q_0 + q_1 i + q_2 j + q_3 k.$$

代入 $qa = bq$ 而比较系数, 得出一次联立方程

$$\begin{aligned}
+(a_1 - b_1)q_1 + (a_2 - b_2)q_2 + (a_3 - b_3)q_3 &= 0,\\
-(a_1 - b_1)q_0 - (a_3 + b_3)q_2 + (a_2 + b_2)q_3 &= 0,\\
-(a_2 - b_2)q_0 + (a_3 + b_3)q_1 - (a_1 + b_1)q_3 &= 0,\\
-(a_3 - b_3)q_0 + (a_2 + b_2)q_1 + (a_1 + b_1)q_2 &= 0.
\end{aligned}$$

此联立方程的行列式等于

$$(a_1^2 + a_2^2 + a_3^2 - (b_1^2 + b_2^2 + b_3^2))^2 = 0,$$

故所求的 q 是存在的.

引理 2 设 $a, b; c, d$ 是两对非零的四元数. 若

$$ab + ba = 0, \quad cd + dc = 0, \quad N(a) = N(c), \quad N(b) = N(d),$$

则有一个四元数 q 使

$$q^{-1}aq = c, \quad q^{-1}bq = d.$$

【证】 由 $ab + ba = 0$ 可知 $-a = b^{-1}ab$, 故 $T(-a) = T(a)$, 即 $T(a) = 0$. 同法证得 $T(b) = T(c) = T(d) = 0$.

由引理 1 可知只而证明 $a = c$ 的情况即是. 即只须证明有一 q 与 a 可交换, 且使 $qbq^{-1} = d$.

用 K 表示由 1 与 a 所演成的域, 即

$$K = \{r + sa; r, s \in F\}.$$

因为 $ab + ba = 0$, 故 b 不在 K 中. 由此可知 $1, a, b, ab$ 对 F 为线性无关. 因之 Q 中的任一元素 d 都可以表成为

$$d = \alpha + b\beta \quad (\alpha, \beta \in K).$$

元素 d 适合 $da = -ad$ 的充分且必要的条件是 $\alpha = 0$, 故

$$d = b\beta, \beta \in K, \text{即} d = b(r_0 + s_0 a) \quad (r_0, s_0 \in F).$$

由 $N(d) = N(b)$ 可知

$$1 = N(r_0 + s_0 a) = r_0^2 + \varepsilon s_0^2 \quad (\varepsilon = N(a) > 0).$$

因 a 与 $r + sa$ 可交换, 故仅需证明有一元素 $r + sa$ 存在, 使

$$(r + sa)b(r_0 + s_0 a)(r + sa)^{-1} = b,$$

即

$$(r - sa)(r_0 + s_0 a) = r + sa.$$

比较系数立得

$$rr_0 + ss_0\varepsilon = r,$$
$$rs_0 - sr_0 = s.$$

其行列式之值为

$$\begin{vmatrix} r_0 - 1 & s_0\varepsilon \\ s_0 & -r_0 - 1 \end{vmatrix} = -(r_0^2 - 1) - s_0^2\varepsilon = 0,$$

故 $q = r + sa$ 是存在的.

定理 2 在一实域上所建成的四元数体的自同构一定是

$$q(a_0^\tau + a_1^\tau i + a_2^\tau j + a_3^\tau k)q^{-1}$$

的形式, 其中 τ 是该实域的自同构, 而 $q \neq 0$.

【证】 命 Q 为所论之四元数体, Q 之中心是一实域 F. 因 Q 的任一自同构一定引出 F 的一个自同构, 故只需证明, 凡 Q 之自同构, 其使 F 的每元皆不变者, 是一内自同构即可. 盖设 σ' 为 Q 的任一自同构, τ 为 σ' 在 F 中所引起的自同构, 则 $\sigma = \sigma'\tau^{-1}$ 显然为 Q 中使 F 之每元皆不变的自同构. 由 $\sigma' = \sigma\tau$, 即明所说. 今设经过此 σ, 把 i 与 j 分别变为 a 与 b, 由 $i^2 = j^2 = -1, ij + ji = 0$ 可知 $a^2 = b^2 = -1, ab + ba = 0$. 但由 $a^2 = -1$, 可知 $N(a)^2 = 1$, 即得 $N(a) = 1$. 同法可得 $N(b) = 1$. 由引理 2, 有一元素 q 存在, 使

$$qaq^{-1} = i, \quad qbq^{-1} = j,$$

故得

$$q\sigma(k)q^{-1} = k,$$

即 σ 是一内自同构.

特别, 当 F 是由所有实数所成的域, 则由定理 2 即得定理 1.

§10 广义四元数体

首先, 我们如下地引入广义四元数体的定义.

设 F 是任意一域, 它的特征数也任意. 设 a 是 F 中的一个非零元素而 $x^2 - x - a$ 是 F 上的不可约 (即不可分解) 多项式 (因此 F 不是代数封闭域, 而 $1 + 4a$ 不是 F 中的平方元素, 如 F 的特征数 $\neq 2$). 将 $x^2 - x - a$ 的一个根 α 添加到 F 之上, 我们得到 F 的一个二次扩域 $F(\alpha)$, 它由一切形状

$$\lambda + \mu\alpha \quad (\lambda, \mu \in F)$$

的元素所组成. $F(\alpha)$ 有唯一的一个自同构

(1) $$\lambda + \mu\alpha \to \overline{\lambda + \mu\alpha} = \lambda + \mu(1 - \alpha),$$

它使 F 中每个元素保持不变, 而不是 $F(\alpha)$ 的单位自同构.

现在在 F 中选取一个非零元素 b, 而 b 不是 $F(\alpha)$ 中元素的平方. 设 β 是另外一个符号, 其意在下文中自明. 考查一切形状

$$x_1 + x_2\beta \quad (x_1, x_2 \in F(\alpha))$$

的元素所组成的集合 Q. 定义

$$x_1+x_2\beta=y_1+y_2\beta,\quad 若 x_1=y_1, x_2=y_2,$$
$$(x_1+x_2\beta)+(y_1+y_2\beta)=(x_1+y_1)+(x_2+y_2)\beta,$$
$$(x_1+x_2\beta)\cdot(y_1+y_2\beta)=(x_1y_1+x_2\bar{y}_2b)+(x_1y_2+x_2\bar{y}_1)\beta.$$

于是 Q 对于这样定义的运算组成一环. 实际上, 除了乘法结合律之外, 其余的环的公理都显然成立, 而乘法结合律可验证如下：

$$\begin{aligned}
&[(x_1+x_2\beta)(y_1+y_2\beta)](z_1+z_2\beta)\\
&\quad=[(x_1y_1+x_2\bar{y}_2b)+(x_1y_2+x_2\bar{y}_1)\beta](z_1+z_2\beta)\\
&\quad=[(x_1y_1+x_2\bar{y}_2b)z_1+(x_1y_2+x_2\bar{y}_1)\bar{z}_2b]\\
&\qquad+[(x_1y_1+x_2\bar{y}_2b)z_2+(x_1y_2+x_2\bar{y}_1)\bar{z}_1]\beta,\\
&(x_1+x_2\beta)[(y_1+y_2\beta)(z_1+z_2\beta)]\\
&\quad=(x_1+x_2\beta)[(y_1z_1+y_2\bar{z}_2b)+(y_1z_2+y_2\bar{z}_1)\beta]\\
&\quad=[x_1(y_1z_1+y_2\bar{z}_2b)+x_2\overline{(y_1z_2+y_2\bar{z}_1)}b]\\
&\qquad+[x_1(y_1z_2+y_2\bar{z}_1)+x_2\overline{(y_1z_1+y_2\bar{z}_2b)}]\beta.
\end{aligned}$$

计算一下就知道 F 是 Q 的中心. 因此, Q 中元素可唯一地表作

$$a_0+a_1\alpha+a_2\beta+a_3\alpha\beta\quad(a_i\in F).$$

我们还可将 $F(\alpha)$ 中的自同构 (1) 扩充成 Q 的一个反自同构：

(2) $$x_1+x_2\beta\to\overline{x_1+x_2\beta}=\bar{x}_1-x_2\beta,$$

即

(3) $$a_0+a_1\alpha+a_2\beta+a_3\alpha\beta\to a_0+a_1(1-\alpha)-a_2\beta-a_3\alpha\beta.$$

显然此反自同构将 F 中元素保持不变. 反之, 如果 F 的特征数 $\neq 2$, 则只有 F 中元素被此反自同构保持不变. 但是当 F 的特征数 $=2$ 时, 一切形状

$$a_0+a_2\beta+a_3\alpha\beta\quad(a_i\in F)$$

的元素皆被此反自同构保持不动.

我们把 Q 称为 F 上的广义四元数环而把 Q 中元素称为广义四元数.

设 $q=a_0+a_1\alpha+a_2\beta+a_3\alpha\beta\in Q$, 定义

$$T(q)=q+\bar{q}=2a_0+a_1,$$
$$N(q)=q\bar{q}=a_0^2+a_0a_1-aa_1^2-ba_2^2-ba_2a_3+aba_3^2,$$

$T(q)$ 称为 q 的迹而 $N(q)$ 称为 q 的范. 显然 $T(q), N(q) \in F$, 对一切 $q \in Q$. 如果 $N(q) \neq 0$, 则 $N(q)^{-1}\bar{q}$ 就是 q 的逆. 因此, Q 是体, 当且仅当 $N(q) \neq 0$, 对一切 $q \neq 0$, 即由

$$a_0^2 + a_0a_1 - aa_1^2 - ba_2^2 - ba_2a_3 + aba_3^2 = 0$$

推出 $a_0 = a_1 = a_2 = a_3 = 0$. 当 Q 是体时, 我们称 Q 为 F 上的广义四元数体.

设 Q 为 F 上的广义四元数体, 则 Q 中任一不属于 F 的元素 q 皆适合一个在 F 上不可约的二次方程

$$x^2 - T(q)x + N(q) = 0.$$

反过来, 我们有

定理 1 设 K 是体, F 是 K 的子域而且 F 包含在 K 的中心之中. 假定 K 中任一不属于 F 的元素都适合一个系数属于 F 的不可约二次方程. 如果 K 不是域, 那么, K 一定是 F 上的广义四元数体.

【证】 首先, 我们断言, 如 K 不是域, 则 $F = F_2$ 这一情形不可能发生. 实际上, 如果 $F = F_2$, 那么一定有 $K = F_2$ 或 $K = F_2(\alpha)$ 是 F_2 的一个二次扩域. 设 $K \neq F_2$, K 中有一个不属于 F_2 的元素 α 存在而 $F_2(\alpha)$ 就是 F_2 的一个二次扩域. 如果 $K \neq F_2(\alpha)$, 那么 K 中就有一个不属于 $F_2(\alpha)$ 的元素 β 存在而 $\beta \notin F_2(\alpha)$, 因之 $\alpha + \beta$ 和 $\alpha\beta$ 都不属于 F_2. 又因为 F_2 中只有一个唯一的不可约二次方程 $x^2 + x + 1 = 0$, 所以由 $\alpha^2 + \alpha + 1 = 0, \beta^2 + \beta + 1 = 0$ 及 $(\alpha + \beta)^2 + (\alpha + \beta) + 1 = 0$ 推出 $\alpha\beta + \beta\alpha = 1$, 于是由 $(\alpha\beta)^2 + \alpha\beta + 1 = 0$ 推出

$$\begin{aligned} 0 &= (\alpha\beta)^2 + (\alpha\beta) + 1 = \alpha(\beta\alpha + 1)\beta + 1 = \alpha^2\beta^2 + 1 \\ &= (\alpha + 1)(\beta + 1) + 1 = \alpha\beta + \alpha + \beta, \end{aligned}$$

所以 $\beta = (\alpha + 1)^{-1}\alpha \in F[\alpha]$, 这与 $\beta \notin F[\alpha]$ 的假设相违.

因此我们一定有 $F \neq F_2$.

其次, 我们断言, 如 K 中任一不属于 F 的元素的平方都属于 F, 那么 K 一定是域. 我们先证明, 这时 K 的特征数一定是 2. 设 α 是 K 中任一不属于 F 的元素, 并设 $\alpha^2 = a \in F$. 于是由 $(\alpha+1)^2 = \alpha^2+2\alpha+1 = 2\alpha+a+1 \in F$ 推出 $2\alpha \in F$. 因 $\alpha \notin F$, 所以 $2\alpha = 0$, 这证明了 K 的特征数 $=2$. 更进一步, 我们证明 K 是域. 实际上, 设 α, β 是 K 中任意两个不属于 F 的元素, $\alpha^2 = a, \beta^2 = b$ 而 $a, b \in F$. 如果 $\beta \in F[\alpha]$, 那么显然有 $\alpha\beta = \beta\alpha$. 如果 $\beta \notin F[\alpha]$, 那么 $\alpha+\beta$ 和 $\alpha\beta$ 都不属于 F. 设 $(\alpha+\beta)^2 = c \in F$, 则 $\alpha\beta+\beta\alpha = a+b+c$, 于是 $(\alpha\beta)^2 = \alpha\beta\alpha\beta = \alpha(\alpha\beta+a+b+c)\beta = ab+(a+b+c)\alpha\beta$. 那么从 $(\alpha\beta)^2 \in F$ 推出 $a+b+c = 0$. 因此这时也有 $\alpha\beta = \beta\alpha$. 所以 K 是域.

因此我们知道如 K 不是域, K 中一定有一个不属于 F 的元素 α 存在, 而 $\alpha^2 \notin F$. 设 α 适合 F 上的不可约二次方程是 $x^2 = ax + b$ $(a, b \in F)$, 而 $a \neq 0$. 令

$\alpha_1 = a^{-1}\alpha$, 那么 α_1 适合 F 上的不可约二次方程 $x^2 = x + a^{-2}b$. 因此, 我们不妨设 K 中有一个不属于 F 的元素 α 适合条件

$$(4) \qquad \alpha^2 = \alpha + a \quad (a \in F).$$

因 $x^2 - x - a$ 不可约, 故 $1 + 4a$ 不是 F 中平方元素, 若 F 的特征数 $\neq 2$. $F(\alpha)$ 有唯一的一个自同构

$$\lambda + \mu\alpha \to \overline{\lambda + \mu\alpha} = \lambda + \mu(1 - \alpha),$$

它使 F 中每个元素保持不变, 而又不是 $F(\alpha)$ 的单位自同构.

如果 $K = F(\alpha)$, 那么 K 是域, 此与 K 不是域的假设相违. 因此 $K \neq F(\alpha)$. 于是 K 中有一个不属于 F 的元素 β 存在而 $\beta \notin F[\alpha]$. 因此 $\alpha + \beta$ 和 $\alpha\beta$ 都不属于 F. 可设 $\beta^2 = b\beta + c$ $(b, c \in F)$. 以 k 表 F 中一个 $\neq 0, 1$ 的元素. 并设

$$\begin{matrix} (\alpha + \beta)^2 = \rho(\alpha + \beta) + \sigma, \\ (\alpha + k\beta)^2 = \lambda(\alpha + k\beta) + \mu, \end{matrix} \quad (\rho, \sigma, \lambda, \mu \in F).$$

于是

$$\alpha\beta + \beta\alpha = (\rho - 1)\alpha + (\rho - b)\beta + \sigma - a - c,$$
$$k(\alpha\beta + \beta\alpha) = (\lambda - 1)\alpha + (\lambda k - k^2 b)\beta + \mu - a - k^2 c,$$

因 $1, \alpha, \beta$ 在 F 上线性无关, 故

$$k(\rho - 1) = \lambda - 1, \quad k(\rho - b) = \lambda k - k^2 b.$$

因 $k \neq 0, 1$, 故 $\rho = b + 1$. 因之

$$\alpha\beta + \beta\alpha = b\alpha + \beta + d \quad (d \in F).$$

命 $\beta_1 = x + y\alpha + \beta$ $(x, y \in F$, 待定$)$. 计算一下可以知道

$$\beta_1^2 = (x^2 + y^2 a + c + yd) + (y^2 + 2xy + yb)\alpha + (b + 2x + y)\beta,$$
$$\alpha\beta_1 + \beta_1\alpha = (2ya + d) + (2x + 2y + b)\alpha + \beta.$$

因此 $\beta_1^2 \in F$ 及 $\alpha\beta_1 + \beta_1\alpha = \beta_1$ 同时成立, 当且仅当

$$\left.\begin{matrix} 2x + y + b = 0, \\ -x + 2ay + d = 0 \end{matrix}\right\}$$

这组线性方程组的行列式等于 $4a + 1 \neq 0$, 因此可以在 F 中求得 x, y, 使得 $\beta_1^2 \in F$ 而 $\alpha\beta_1 + \beta_1\alpha = \beta_1$. 因此我们不妨设 K 中有不属于 F 的元素 β 存在, $\beta \notin F[\alpha]$ 而且

$$(5) \qquad \beta^2 = b, \alpha\beta + \beta\alpha = \beta,$$

其中 b 是 F 中非平方元素. 令 Q 表 K 中一切形如

$$a_0 + a_1\alpha + a_2\beta + a_3\alpha\beta \quad (a_i \in F)$$

的元素的集合, 则 Q 是 F 上的广义四元数体, 而 Q 有反自同构

$$\begin{aligned} a_0 + a_1\alpha + a_2\beta + a_3\alpha\beta \to \overline{a_0 + a_1\alpha + a_2\beta + a_3\alpha\beta} \\ = a_0 + a_1(1-\alpha) - a_3\beta - a_3\alpha\beta. \end{aligned}$$

最后, 我们证明 $K = Q$. 如果 $K \neq Q$, 则有 $\gamma \in K$ 而 $\gamma \notin Q$. 像前面一样, 我们不妨假定

$$\gamma^2 = c, \quad \alpha\gamma + \gamma\alpha = \gamma,$$

其中 c 是 F 中非平方元素. 可以设

$$\begin{matrix} (\beta+\gamma)^2 = \rho_1(\beta+\gamma) + \sigma_1 \\ (\beta+k\gamma)^2 = \lambda_1(\beta+k\gamma) + \mu_1, \end{matrix} \quad (\rho_1, \sigma_1, \lambda_1, \mu_1 \in F).$$

于是

$$\begin{aligned} \beta\gamma + \gamma\beta = \rho_1\beta + \rho_1\gamma + \sigma_1 - b - c, \\ k(\beta\gamma + \gamma\beta) = \lambda_1\beta + \lambda_1 k\gamma + \mu_1 - b - ck^2. \end{aligned}$$

因 $1, \beta, \gamma$ 在 F 上线性无关, 故

$$k\rho_1 = \lambda_1, \quad k\rho_1 = \lambda_1 k.$$

因 $k \neq 0, 1$, 故 $\lambda_1 = \rho_1 = 0$. 因之可设

$$\beta\gamma + \gamma\beta = d \in F.$$

又因 $(\alpha\beta)^2 = -ab$, 故同理可设

$$(\alpha\beta)\gamma + \gamma(\alpha\beta) = f \in F.$$

于是

$$\begin{aligned} (\alpha\beta)\gamma &= f - \gamma(\alpha\beta) = f - (\gamma\alpha)\beta = f - (\gamma - \alpha\gamma)\beta \\ &= f - \gamma\beta + (\alpha\gamma)\beta = f - (d - \beta\gamma) + \alpha(\gamma\beta) \\ &= f - d + \beta\gamma + \alpha(d - \beta\gamma) = (f-d) + d\alpha + \beta\gamma - \alpha(\beta\gamma). \end{aligned}$$

因此

$$(2\alpha\beta - \beta)\gamma = (f-d) + d\alpha,$$

因 $2\alpha\beta-\beta\neq 0$, 故

$$\gamma=(2\alpha\beta-\beta)^{-1}(f-d+d\alpha)\in Q.$$

我们得到一个矛盾. 定理 1 至此完全证毕.

从定理 1 的证明看出, 我们实际上证明了

定理 2 设 K 是体, F 是 K 的子域而且 F 包含在 K 的中心之中. 假设 K 中任一不属于 F 的元素都适合一个系数属于 F 的不可约二次方程, 那么, K 只有以下几种可能:

I. $K=F$ 或 $K=F(\alpha)$ 是 F 的一个二次扩域;

II. K 是由特征数为 2 的域 F 添加一些 F 中元素的平方根所得;

III. K 是 F 上广义四元数体.

§11 体的性质

定理 1 一体中如有一中心以外的元素, 则此体可由该元素之诸共轭元素演出之.

【证】 吾人易见, 若 $ab\neq ba$, 则

$$a=(b-(a-1)^{-1}b(a-1))(a^{-1}ba-(a-1)^{-1}b(a-1))^{-1}. \tag{1}$$

命 K 为一体, L 为由所说元素之诸共轭元素所成之组. 设 K_1 是 L 所演成的体. 由 (1) 可知, 若 a 与 L 中之一元素, 如 b, 不可交换, 则 a 必在体 K_1 中, 即 $K\setminus K_1$ 之任一元素与 K_1 之任一元素都是可交换的.

假定此定理不成立, 即有一元素 c 在 $K\setminus K_1$ 中, 由 K_1 之定义, 在 K_1 中有二元素 b 与 b' 使 $bb'\neq b'b$. 因 c, cb 都在 $K\setminus K_1$ 中, 故 $(cb)b'=b'(cb)=cb'b$, 此与 $bb'\neq b'b$ 相矛盾. 定理即以证明.

由此定理, 吾人可得出若干推论.

定义 1 设 K_1 为 K 之一子体. 若 K_1 经 K 的所有内自同构皆不变, 则称 K_1 为 K 之一正规子体.

定理 2 一体的正规子体 (非自己) 必包在中心之中.

此乃定理 1 之另一说法而已.

定义 2 设 G 为群, G 中二元素 a,b 的换位子定义为 $(a,b)=aba^{-1}b^{-1}$, 一 r 级的换位子是用归纳法由

$$(a_1,a_2,\cdots,a_r)=(a_1(a_2,\cdots,a_r))$$

来定义.

定理 3　任一非域之体之换位子演出此体.

由 $a(b,c)a^{-1}=(a,(b,c))(c,b)^{-1}$, 可知换位子演出之体显然为该体之一正规子体, 故吾人只须证明, 换位子不可能都在中心中. 设 a 不在中心中, 在此体中选择元素 b 使 $ab\neq ba$, 将公式 (1) 稍加变化, 即得

$$a=(1-(a-1)^{-1}b^{-1}(a-1)b)\cdot(a^{-1}b^{-1}ab-(a-1)^{-1}b^{-1}(a-1)b)^{-1}. \tag{2}$$

由此等式可知 $a^{-1}b^{-1}ab$ 及 $(a-1)^{-1}b^{-1}(a-1)b$ 之一不在中心之中.

定理 4　如果一体的中心包有所有的换位子, 此体必为一域. 如果一体中之一元素和所有的换位子都是可交换的, 此元素一定在中心中.

为了进一步了解体的性质, 我们应当进而研究体的乘法群的性质, 怎样的群才能作为体的加法群? 这是一个极饶趣味的问题, 除掉若干特例之外, 我们所知极少.

定义 3　对于群 G, 有一中心 G_1, 作商群 G/G_1, 亦应该有中心 G_2/G_1, 这 G_2 对 G 是正规的, 于是又可以作商群 G/G_2, 也可考查其中心, 这样继续下去, 得到一个群列:

$$\{1\}\subseteq G_1\subseteq G_2\subseteq\cdots\subseteq G_n\subseteq\cdots,$$

我们称此为上中心群列.

定理 5　设 G 为体 K 的乘法群, G_1 为其中心, 则 G/G_1 除了单位元素之外, 就没有其他的中心元素了, 即上中心群列如下:

$$\{1\}\subseteq G_1\subseteq G_1\subseteq G_1\subseteq\cdots.$$

【证】　若 K 是域, 则此定理显然成立, 且 $G_1=G$. 若 K 不是域. 而 G/G_1 中有一个非单位的中心元素 A. 命 $A=aG_1$(a 为 A 中的代表, 而 $a\notin G_1$).

由

$$aG_1bG_1=bG_1aG_1$$

可知 $a^{-1}b^{-1}ab\in G_1$, 即对于所有的 $b\in G, a^{-1}b^{-1}ab\in G_1$. 由于 a 不在 G_1 中, 故可取 G 之一元素 b, 使

$$ab\neq ba.$$

由等式 (2),

$$b=(1-\mu)(\mu-\lambda)^{-1}\quad(\lambda,\mu\in G_1),$$

得出矛盾. 故定理证毕.

定义 4　设 G 为群, 再设 G' 及 G'' 是 G 的子群. 用 $[G',G'']$ 表示由所有 G' 中的元素 a 与 G'' 中的元素 b 的换位子演出的群, 我们利用归纳法来定义

$$G_1=G,\quad G_2=[G,G_1],\cdots,\quad G_n=[G,G_{n-1}],\cdots.$$

显然有

$$G_1 \supseteq G_2 \supseteq \cdots \supseteq G_n \supseteq \cdots,$$

此序列称为群 G 的下中心群列.

我们再定义

$$G^{(0)} = G, \quad G^{(1)} = [G^{(0)}, G^{(0)}], \cdots, \quad G^{(n)} = [G^{(n-1)}, G^{(n-1)}], \cdots.$$

显然有

$$G^{(0)} \supseteq G^{(1)} \supseteq G^{(2)} \supseteq \cdots \supseteq G^{(n)} \supseteq \cdots,$$

此序列称为群 G 的导来群列.

若存在一自然数 n, 使 $G^{(n-1)} = \{1\}$, 则 G 被称为亚 Abel 群.

定理 6 设非交换体 K 的乘法群为 G, 则 G_ν 经过体的运算演出体 K.

【证】 当 $\nu = 2$ 时, 就是定理 3. 现在用归纳法来证明. 假定此定理对 ν 已成立. 故 G_ν 中有二元素 a, b, 使 $ab \neq ba$. 由 (2) 可知 $G_{\nu+1}$ 中亦有一不属于中心的元素, 因为 $G_{\nu+1}$ 是 G 的正规子群, 故由定理 1 可知 $G_{\nu+1}$ 也演出体 K.

本定理建议了一个值得研究的问题: 下中心群列是否经常下降, 即能否到某一步之后, 就相等了.

〔例〕 实数域上的四元体有

$$G_1 \supseteq G_2 = G_3 = \cdots$$

的性质.

定理 7 一体的乘法群如果不是 Abel 群, 就也不是亚 Abel 群. 换一句话说, 一个非域的体的乘法群的导来群列不会终于 $\{1\}$ 的.

要证明这条定理, 我们需要以下的两条引理:

引理 1 设 $\Delta = Z(x, y)$ 是一体, 是由中心 Z 添入二元素 x 及 y 所得者. 若

$$xy = \gamma yx,$$

此 $\gamma \neq 1$ 但在 Z 中, 则 x 对 Z 是代数的必要且充分条件为 γ 是一单位根.

【证】 若 γ 是一 $q(>1)$ 次单位根, 则 x^q 与 y 可交换, 即 x^q 在中心之中, 亦即 x 对 Z 是代数的.

若 x 对 Z 是代数的, 设 x 所适合的最低次方程为

$$f(x) = a_k x^k + \cdots + a_1 x + a_0 = 0 \quad (a_k \neq 0, a_i \in Z). \tag{3}$$

用 y 来变换 (3) 式, 即得

$$y^{-1} f(x) y = a_k \gamma^k x^k + \cdots + a_1 \gamma x + a_0 = 0. \tag{4}$$

若 (3) 与 (4) 不完全相同, 即将其相减, 可得出一方程式, 其系数在 Z 中, 其次数小于 k. 这和假设相违背. 因之可知

$$a_k(\gamma^k - 1) = 0,$$

即 $\gamma^k = 1$.

引理 2 设 K 表一体, 其中有二元素 x 与 y 适合于 $xy = \gamma yx$, 此 γ 在中心中, 定义

$$x_1 = (y, 1-x) = y^{-1}(1-x)^{-1}y(1-x) = (1-\gamma x)^{-1}(1-x),$$
$$x_l = (y, x_{l-1}).$$

则有

$$x_l = x_l(x) = \prod_{t=0}^{l}(1-\gamma^t x)^{(-1)^t\binom{l}{t}}. \tag{5}$$

【证】 当 $l=1$, 此引理显然成立. 假定其对 $l-1$ 成立, 则

$$\begin{aligned} x_l &= y^{-1}x_{l-1}^{-1}yx_{l-1} = (x_{l-1}(\gamma x))^{-1}x_{l-1}(x) \\ &= \prod_{t=1}^{l}(1-\gamma^t x)^{(-1)^t\binom{l-1}{t-1}}\prod_{t=0}^{l-1}(1-\gamma^t x)^{(-1)^t\binom{l-1}{t}} \\ &= \prod_{t=0}^{l}(1-\gamma^t x)^{(-1)^t\binom{l}{t}}. \end{aligned}$$

故对 l, (5) 式亦真. 此即证明了引理 2.

【定理 7 的证明】 设 K 表所论的体, Z 是其中心. 今只须证明, 若 K 中有一元素不在 Z 中, 则 K 的乘法群不是亚 Abel 群.

设 G 为 K 的乘法群, $G^{(r)}(r=0,1,2,\cdots)$ 是第 r 个导来群. 今用归纳法来证明所有的 $G^{(r)}(r=1,2,\cdots)$ 都不在 Z 中. $G^{(0)}=G$ 假定不在 Z 中.

假定 $G^{(0)},\cdots,G^{(r-1)}$ 都不在 Z 中, 而 $G^{(r)}$ 在 Z 中. 命

$$a, b, \cdots \quad (\text{不一定是可数的})$$

是 $G^{(r)}$ 对 $G^{(r-1)}$ 的傍系 (即陪集) 的代表, 因 $G^{(r-1)}$ 是 G 的正规子群, 故由定理 2, $G^{(r-1)}$ 演出体 K, 即

$$K = Z(a, b, \cdots),$$

此处 $a, b, \cdots$ 在 $G^{(r-1)}$ 中, 但 $(a, b), \cdots$ 却在 $G^{(r)}$ 中, 即在 Z 中. 因 K 是不可交换的, 故可从其中取出两个元素 x, y, 使

$$(x, y) = \gamma,$$

但 $\gamma \neq 1$ 而在 Z 中.

由引理 2 中 x_l 的定义可知, 当 $l \geqslant r$ 时, x_l 在 $G^{(r)}$ 中, 盖 y 与 $x_s(s<r)$ 各在 $G^{(r-1)}$ 及 $G^{(s)}$ 之中也. 今分两种情形来进行讨论:

I. γ 非单位根. 由引理 1, x 对 Z 是超越的, 则对 $l \geqslant r$ 有

$$x_l = \prod_{t=0}^{l}(1-\gamma^t x)^{(-1)^t\binom{l}{t}}$$

不能在 Z 中. 盖若不然, 则由

$$x_l \prod_{0<2t+1\leqslant l}(1-\gamma^{2t+1}x)^{\binom{l}{2t+1}} = \prod_{0\leqslant 2t\leqslant l}(1-\gamma^{2t}x)^{\binom{l}{2t}},$$

比较两边的常数项及 x 的系数可知

$$x_l = 1$$

及

$$\sum_{0<2t+1\leqslant l}\begin{pmatrix} l \\ 2t+1 \end{pmatrix}\gamma^{2t+1} = \sum_{0\leqslant 2t\leqslant l}\begin{pmatrix} l \\ 2t \end{pmatrix}\gamma^{2t},$$

此式可改写为

$$\sum_{t=0}^{l}(-1)^t\begin{pmatrix} l \\ t \end{pmatrix}\gamma^t = (1-\gamma)^l = 0,$$

此为不可能者.

II. 若 γ 是 1 的 q 次原根. 我们考虑体 $\Delta = Z(x,y)$. 命 Z_1 是 Δ 的中心, 显然 $Z_1 \supseteq Z$, 故 $\Delta = Z_1(x,y)$. 若 Z_1 仅有有限个元素, 由引理 1, x 及 y 对 Z_1 是代数的, 故 Δ 是一有限体; 由定理 6.7 可知 Δ 是一域, 这与 $xy \neq yx$ 相违背. 故 Z_1 有无限多个元素. 因 x^q 与 y 可交换, 且在 Z_1 中, 故

$$x^q = \alpha \quad (\alpha \in Z_1),$$

此为 x 所满足的、系数属于 Z 的最低次方程. 盖若不然, 设 x 所适合的最低次方程式的次数 $q' < q$, 则

$$f(x) - y^{-1}f(x)y = f(x) - f(\gamma x) = 0,$$

即得 $\gamma^{q'} = 1$, 与 γ 是一 q 次原根的假设相违.

因 $xy = \gamma yx$, 对所有的 $a \in Z_1$, 有

$$(ax)y = \gamma y(ax),$$

由引理 2 有

$$x_l = x_l(ax) = \prod_{m=0}^{l}(1-\gamma^m ax)^{(-1)^m\binom{l}{m}}$$
$$= \prod_{t=0}^{q-1}(1-\gamma^t ax)^{\lambda_t},$$

其中

$$\lambda_t = \sum_{0\leqslant t+qs\leqslant l}(-1)^{t+qs}\binom{l}{t+qs}.$$

当 $l \geqslant r$ 时, $x_l(ax)$ 在中心 Z_1 中, 且

$$\prod_{t=0}^{q-1}(1-\gamma^t ax) = 1-(ax)^q = 1-\alpha a^q$$

亦在中心中.

命

$$-N = \min_{0\leqslant t\leqslant q-1}\lambda_t.$$

因为

$$\sum_{t=0}^{q-1}\lambda_t = \sum_{t=0}^{l}(-1)^t\binom{l}{t} = 0,$$

故 N 是一非负整数. 命

(6)
$$x_l(ax)(1-\alpha a^q)^N = \prod_{t=0}^{q-1}(1-\gamma^t ax)^{\lambda_t+N}$$
$$= A_0(a)+A_1(a)x+\cdots+A_{q-1}(a)x^{q-1},$$

此处 $A_1(a)$ 中 a 的系数为

(7)
$$\sum_{t=0}^{q-1}(\lambda_t+N)\gamma^t = \sum_{t=0}^{q-1}\lambda_t\gamma^t = \sum_{t=0}^{l}(-1)^t\binom{l}{t}\gamma^t = (1-\gamma)^l \neq 0.$$

故 (6) 式之左边在 Z_1 中, x 适合一方程式其次数 $< q$, 故对所有的 $a\in Z_1$, 常有

$$A_1(a) = 0.$$

因 Z_1 有无限多个元素, 而 $A_1(a)$ 的系数必全为零, 故 $A_1(a)$ 中 a 的系数亦为零, 此与 (7) 相矛盾. 故定理证毕.

与定理 7 完全等价有

定理 8　一体的乘法群的 r 次导来群演出此体.

第二章　一维射影几何及二级线性群

§1　射影空间及群

假定 K 是一个体. 我们现在研究 K 内有序的元素对 (x_1, x_2), 或简称为序偶, 并假定 x_1 与 x_2 不同时为零.

如果存在有 K 中一非零元素 ρ, 使 $x_1 = \rho y_1, x_2 = \rho y_2$, 则两序偶 (x_1, x_2) 与 (y_1, y_2) 称为等价, 并写成

$$(x_1, x_2) = \rho(y_1, y_2).$$

这个等价关系显然有以下三性质: (i) 一序偶与其自己等价; (ii) 若 (x_1, x_2) 与 (y_1, y_2) 等价, 则 (y_1, y_2) 与 (x_1, x_2) 等价; (iii) 若 (x_1, x_2) 与 (y_1, y_2) 等价, (y_1, y_2) 与 (z_1, z_2) 等价, 则 (x_1, x_2) 与 (z_1, z_2) 等价.

依此等价关系把序偶分类: 每一类中的诸元素都等价; 不同类的元素必不等价.

一个序偶类称为一点, 这种点的全体称为体 K 上的一维射影空间或射影直线. 故一点有很多个序偶与之对应, 其中之任一都称为此点的齐次坐标. 如果 $x_2 \neq 0$, 则 $x = x_2^{-1} x_1$ 就称为此点的非齐次坐标. 仅有一类, 其中 $x_2 = 0$, 这类所代表的点称为无穷远点, 用符号 ∞ 来表示它的非齐次坐标. 所以 K 上的一维射影空间就是 K 的所有元素加上无穷远点所得的集合.

命

$$M = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$$

表示一个二级可逆方阵. 今后命

$$M^{-1} = \begin{pmatrix} a' & b' \\ c' & d' \end{pmatrix}$$

为适合

(1)
$$\begin{pmatrix} a & b \\ c & d \end{pmatrix}\begin{pmatrix} a' & b' \\ c' & d' \end{pmatrix} = \begin{pmatrix} a' & b' \\ c' & d' \end{pmatrix}\begin{pmatrix} a & b \\ c & d \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$$

的矩阵.

我们定义

(2)
$$(x_1, x_2) = \rho(y_1, y_2)M$$

为一维射影空间中的一个射影变换, 也就是

$$(3)\qquad \begin{cases} x_1=\rho(y_1a+y_2c), \\ x_2=\rho(y_1b+y_2d). \end{cases}$$

不难验证, 这是一个把射影空间变为其自身的一一变换. 射影变换的全体组成一群, 称为 K 上一维射影群, 记之为 $PGL_2(K)$.

如果我们用非齐次坐标, 则 (3) 式变为

$$(4)\qquad x=x_2^{-1}x_1=(yb+d)^{-1}(ya+c).$$

再借助于 (1) 式, 由直接验算可知

$$(ya+c)(-b'y+a')=(yb+d)(d'y-c'),$$

因此我们可得

$$(5)\qquad x=(d'y-c')(-b'y+a')^{-1}.$$

注意, (4) 与 (5) 式把 $y=-db^{-1}=b'^{-1}a'$ 变为无穷远点 $x=\infty$, 并把无穷远点 ∞ 变为 $b^{-1}a=-d'b'^{-1}$(如果 $b\neq 0$). 如果 $b=0$, 则 (4) 式变为

$$x=d^{-1}(ya+c),$$

这一变换使无穷远点不变. 因此我们不妨约定, 对 K 中所有的 a 恒有

$$\infty+a=\infty,\quad a\cdot\infty=\infty\cdot a=\infty,$$
$$a\cdot 0^{-1}=0^{-1}\cdot a=\infty,$$
$$a\cdot\infty^{-1}=\infty^{-1}\cdot a=0.$$

注意, 以上所述, 我们定义了一维"左"射影空间, 似乎还可定义一维"右"射影空间. 我们现在必须说明一维左射影空间和一维右射影空间是一回事. 左空间中以 (x_1,x_2) 为齐次坐标的点和右空间中以 $\begin{pmatrix} x_1' \\ x_2' \end{pmatrix}$ 为齐次坐标的点是同一点的两个不同形式, 如果它们适合等式 $x_1\cdot x_2'=x_2\cdot x_1'$ 的话. 这时它们有同一非齐次坐标 $x=x_2^{-1}\cdot x_1=x_1'\cdot x_2'^{-1}$.

定理 1　命 $GL_2(K)$ 表 K 上所有 2×2 可逆矩阵所组成的群, 命 Z_2 表其中心, 则 Z_2 由一切形如

$$(6)\qquad \lambda I$$

的元素所组成, 其中 $\lambda \in Z^*, Z^*$ 表 Z 的乘法群, 而且

$$PGL_2(K) \cong GL_2(K)/Z_2.$$

【证】 $GL_2(K)$ 包有形如

$$\begin{pmatrix} a & 0 \\ 0 & a \end{pmatrix} \quad (a \in K^*)$$

的元素, K^* 表 K 的乘法群. 与这些元素可交换的二级矩阵的形状是

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix},$$

此处 a, b, c, d 在 K 的中心 Z 之中. 又如果它与

$$\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}, \quad \begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix}$$

可交换, 则它一定是 (6) 的形状.

其次, 若

$$M = \lambda N,$$

此处 $\lambda \in Z^*$, 则显然 (2) 可写成

$$(x_1, x_2) = \rho\lambda(y_1, y_2)N,$$

故 M 与 N 表同一射影变换.

最后, 我们需证的是: 如果 M 与 N 表同一射影变换, 则有一中心元素 λ, 使 $M = \lambda N$. 若

$$(x_1, x_2) = \rho(y_1, y_2)M = \rho'(y_1, y_2)N,$$

则

$$(y_1, y_2) = \rho^{-1}\rho'(y_1, y_2)NM^{-1}.$$

故仅需证使每一点不变的变换的形状是 $M = \lambda I$, 其中 $\lambda \in Z^*$ 即可. 取 $(0,1), (1,0)$ 及 $(1, 1)$ 三点, 得

$$M = \begin{pmatrix} a & 0 \\ 0 & a \end{pmatrix},$$

这个变换的非齐次形式是 $x = a^{-1}ya$. 由 $x = a^{-1}xa$ 可知 a 属于 K 的中心. 于是定理证毕.

以下我们将首先研究群 $PGL_2(K)$ 的可迁性.

定理 2 射影直线上的任何真子集都可用一适当的射影变换变到一个不含无穷远点的子集.

【证】 如果这个真子集不含无穷远点, 则单位变换就适合定理的要求, 而如果这个真子集包有无穷远点而不含有点 a, 则

$$x = (y-a)^{-1}$$

这个变换就适合定理的要求.

定理 3 $PGL_2(K)$ 是可迁群 (即对射影直线上任意两点 a, b, 都存在射影变换把 a 变到 b).

【证】 只要能够证明有射影变换将任何有限点 a 变到 ∞ 即可. 显然, 射影变换

$$x = (y-a)^{-1}$$

是将点 a 变到无穷远点的, 因而定理得证.

定理 4 $PGL_2(K)$ 中仅将一固定点不变的子群与下列变换

$$x = ayb + c$$

所组成的群 (称为空间的仿射群) 同构.

【证】 由定理 3, 我们只要证明将 ∞ 点不变的变换之全体组成的群与上述的群同构就行了, 而这只要在 $x = (yb+d)^{-1}(ya+c)$ 中令 $b = 0$ 就行了.

定理 5 $PGL_2(K)$ 双可迁 (即对任意两点 a, b, 存在射影变换使它们变到任意指定的两点 c, d).

【证】 与定理 3 证明的类似理由, 仅需证明任意一对点 a, b 都可以用一个射影变换使它们依序变到 ∞, 0 两点即行. 事实上, 这个变换是存在的, 因为依定理 3 有一个射影变换 T_1 存在, 它将点 a 变到 ∞, 而将点 b 变到某一点 c, 以 T_2 表变换 $x = y - c$, 则 $T_1 \cdot T_2$ 就将 a 变到 ∞ 而将 b 变到 0, 因而定理得证.

定理 6 $PGL_2(K)$ 中将两个固定点不变的变换所组成的群与下列形式的变换:

$$x = ayb$$

所组成的群 (称为等价群) 同构.

【证】 与定理 4 类似的理由, 由于 $x = ayb$ 是使 ∞ 和 0 两点不变的射影变换, 因而知本定理成立.

定理 7 $PGL_2(K)$ 三可迁 (即任意三点都可变到任意指定的三点).

【证】 只要证明给了任意三点, 都可找到一个射影变换 T, 使 $aT = \infty, bT = 0, cT = 1$. 事实上, 依定理 5, 有一个射影变换 T_1 存在, 使 $aT_1 = \infty, bT_1 = 0$. 假定 $cT_1 = d$. 令 T_2 表变换 $x = d^{-1}y$, 则 $T = T_1T_2$ 即适合要求, 因而定理证毕.

定理 8 $PGL_2(K)$ 中将三个固定点不变的子群与下列形式的变换:

$$x = aya^{-1}$$

所组成的群 (称为相似变换群) 同构.

【证】 由于 $x = aya^{-1}$ 恰是使 $0, 1, \infty$ 三点不变的射影变换, 因而知定理成立.

令以 σ 表 K 的任意半自同构, 则变换

$$x = (y^\sigma b + d)^{-1}(y^\sigma a + c)$$

称为射影直线的广义射影变换, 射影直线上的广义射影变换之全体组成一群称为广义射影群.

§2 调和点列和一维射影几何的基本定理

在本节中我们将证明特征数 $\neq 2$ 的体上的一维射影几何的基本定理 (定理 1 及定理 2). 首先我们定义

定义 以 x_1, x_2, x_3 和 x_4 表射影直线上的四个点, 称它们组成一个调和点列, 如果有

$$(x_2 - x_4)^{-1}(x_2 - x_3)(x_1 - x_3)^{-1}(x_1 - x_4) = -1. \tag{1}$$

定理 1 射影直线上的广义射影变换必将调和点列变到调和点列.

【证】 任意广义射影变换都是一个射影变换和一个半自同构的乘积, 因此只需要对这两种变换来证明本定理就行.

第一种变换. 设 $x = (yb + d)^{-1}(ya + c)$ 为一射影变换, 则应用 (1.4) 与 (1.5) 就有

$$\begin{aligned}x_i - x_j =&(y_ib + d)^{-1}(y_ia + c) - (d'y_j - c')(-b'y_j + a')^{-1}\\ =&(y_ib + d)^{-1}[(y_ia + c)(-b'y_j + a')\\ &- (y_ib + d)(d'y_j - c')](-b'y_j + a')^{-1}\\ =&(y_ib + d)^{-1}(y_i - y_j)(-b'y_j + a')^{-1}.\end{aligned}$$

于是

$$
\begin{aligned}
&(x_2-x_4)^{-1}(x_2-x_3)(x_1-x_3)^{-1}(x_1-x_4)\\
=&(-b'y_4+a')(y_2-y_4)^{-1}(y_2-y_3)(y_1-y_3)^{-1}\\
&\cdot(y_1-y_4)(-b'y_4+a')^{-1}.
\end{aligned}
$$

因此, 如果 x_1,x_2,x_3,x_4 组成一调和点列, 则经一射影变换所得的四点亦然.

第二种变换. 设 σ 为半自同构, 由第一章 §4 定理 1 知 σ 或为自同构或为反自同构. 当 σ 为自同构时定理显然成立. 今证 σ 为反自同构的情形.

首先, 我们有等式

$$a^{-1}(a\pm b)b^{-1}=b^{-1}(a\pm b)a^{-1}, \tag{2}$$

其中 a,b 为 K 中任意两个非零元素. 由 (1) 两边各左乘 $(x_2-x_1)^{-1}\cdot(x_2-x_4)$, 右乘 $(x_1-x_4)^{-1}$, 得

$$
\begin{aligned}
&(x_2-x_1)^{-1}(x_2-x_3)(x_1-x_3)^{-1}\\
&=-(x_2-x_1)^{-1}(x_2-x_4)(x_1-x_4)^{-1}.
\end{aligned}\tag{3}
$$

应用等式 (2) 于 (3) 式的两边得

$$
\begin{aligned}
&(x_1-x_3)^{-1}(x_2-x_3)(x_2-x_1)^{-1}\\
&=-(x_1-x_4)^{-1}(x_2-x_4)(x_2-x_1)^{-1}.
\end{aligned}\tag{4}
$$

由 (4) 式两边各左乘 (x_1-x_4) 右乘 $(x_2-x_1)(x_2-x_4)^{-1}$ 得

$$(x_1-x_4)(x_1-x_3)^{-1}(x_2-x_3)(x_2-x_4)^{-1}=-1. \tag{5}$$

将反自同构 σ 作用于 (5) 式两边就得出

$$(x_2^\sigma-x_4^\sigma)^{-1}(x_2^\sigma-x_3^\sigma)(x_1^\sigma-x_3^\sigma)^{-1}(x_1^\sigma-x_4^\sigma)=-1.$$

这就是说, $x_1^\sigma,x_2^\sigma,x_3^\sigma,x_4^\sigma$ 也组成一个调和点列, 至此定理证毕.

反之, 我们有

定理 2　射影直线上的一个一一变换将调和点列变到调和点列者必为广义射影变换.

【证】　设 T 是这样的一个变换, 则依定理 1.7 知有一个射影变换 ρ 存在, 使得 $T\rho$ 将 $0,1,\infty$ 三点不变. 此 ρ 当然是一个广义射影变换, 且 $T\rho$ 仍是使调和点

列变到调和点列的一个一一变换. 因广义射影变换全体成群, 所以我们仅需证明将 $0, 1, \infty$ 三点不变且将调和点列变到调和点列者必为广义射影变换就行了. 设 τ 为这样的一个变换, 我们将证明 τ 是 K 的一个半自同构.

以 x^τ 表点 x 在 τ 之下的像, 则由假设知

$$0^\tau = 0, \quad 1^\tau = 1, \quad \infty^\tau = \infty.$$

设 x, y 为 K 中任意两个元素, 令

$$x_1 = 2x, \quad x_2 = 2y.$$

而且令

(6) $$x_3 = \frac{1}{2}(x_1 + x_2),$$

则

$$(x_2 - x_3)(x_1 - x_3)^{-1} = -1,$$

因此 x_1, x_2, x_3, ∞ 四点组成调和点列, 因 τ 将调和点列变到调和点列, 所以我们有

$$(x_2^\tau - x_3^\tau)(x_1^\tau - x_3^\tau)^{-1} = -1,$$

于是

(7) $$x_3^\tau = \frac{1}{2}(x_1^\tau + x_2^\tau).$$

由 (6) 及 (7) 可推出

$$\left[\frac{1}{2}(x_1 + x_2)\right]^\tau = \frac{1}{2}(x_1^\tau + x_2^\tau),$$

即

$$(x + y)^\tau = \frac{1}{2}[(2x)^\tau + (2y)^\tau],$$

当 $y = 0$ 时我们有

$$x^\tau = \frac{1}{2}(2x)^\tau,$$

因此就有

(8) $$(x + y)^\tau = x^\tau + y^\tau.$$

如果令 $x_1 = x, x_2 = 1 - x$, 取 x_3 使 $x_1, x_2, x_3, 0$ 四点组成调和点列, 因而 $x_3 = 2x_1x_2$. 由 $x_1^\tau, x_2^\tau, x_3^\tau, 0$ 仍是调和点列得 $x_3^\tau = 2x_1^\tau \cdot x_2^\tau$, 所以

$$[2x(1 - x)]^\tau = 2x^\tau(1 - x)^\tau.$$

于是

$$x^\tau - (x^2)^\tau = x^\tau - (x^\tau)^2,$$

即

$$(x^2)^\tau = (x^\tau)^2.$$

于是

$$\begin{aligned}(xy + yx)^\tau &= [(x+y)^2 - x^2 - y^2]^\tau \\ &= [(x+y)^\tau]^2 - (x^\tau)^2 - (y^\tau)^2 = x^\tau y^\tau + y^\tau x^\tau,\end{aligned}$$

因此由第一章 §4 定理 3 知 τ 为半自同构, 所以此变换为广义射影变换. 定理证毕.

§3 射影对合

定义 1　设 a, b 为射影直线上任意两定点, 一个依下列法则:

(1)
$$(x, y, a, b) = -1$$

即

(2)
$$(y-b)^{-1}(y-a)(x-a)^{-1}(x-b) = -1$$

将 y 变到 x 的变换显然是一个射影变换, 这种射影变换称为第一种射影对合, 点 a 和点 b 在变换 (1) 之下不变, 称为第一种射影对合 (1) 的固定点.

显然, 第一种射影对合由它的固定点所唯一决定. 如果在 (1) 中令 $a = 0, b = \infty$, 则第一种射影对合就取下列形状:

(3)
$$x = -y,$$

因而其矩阵为

$$\begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}.$$

一般说来, 任何第一种射影对合在相似变换之下, 都可以化成这种形状. 实际上, (1) 的矩阵是

$$\begin{pmatrix} 1 & 1 \\ -b & -a \end{pmatrix}\begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}\begin{pmatrix} 1 & 1 \\ -b & -a \end{pmatrix}^{-1}.$$

定理 1 一非中心矩阵 M 表一第一种射影对合的充要条件为有一中心元素 λ 存在, 使

$$(\lambda M)^2 = I.$$

这个定理的证明有赖于以下纯代数的引理.

引理 1 设 M 为非中心可逆矩阵, 则 $M^2 = I$ 成立, 当且仅当有一可逆矩阵 P 存在, 使得

$$M = P^{-1}\begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}P.$$

【证】 如果 $M = P^{-1}\begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}P$, 则显然有 $M^2 = I$. 反之, 设 $M^2 = I$, 将 M 写成

$$M = \begin{pmatrix} a & b \\ c & d \end{pmatrix}, \tag{4}$$

则由 $M^2 = I$ 得出

$$\begin{cases} a^2 + bc = cd + d^2 = 1, \\ ab + bd = ca + dc = 0. \end{cases} \tag{5}$$

我们分三个情形来讨论:

(i) $b = c = 0$, 则 $a^2 = d^2 = 1$. 因 M 不是中心矩阵, 所以必须 $a = 1, d = -1$ 或 $a = -1, d = 1$. 在前一种情形有

$$M = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix},$$

因之, 可取单位矩阵 I 作为 P. 在后一种情形有

$$M = \begin{pmatrix} -1 & 0 \\ 0 & 1 \end{pmatrix},$$

这时

$$\begin{pmatrix} -1 & 0 \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}^{-1}\begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}\begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}.$$

(ii) $b \neq 0$. 由 (5) 中解出 c 和 d:

$$c = b^{-1}(1 - a^2), \quad d = -b^{-1}ab.$$

于是

$$M=\begin{pmatrix} a & b \\ b^{-1}(1-a^2) & -b^{-1}ab \end{pmatrix}$$

$$=\begin{pmatrix} 1 & 0 \\ 0 & b^{-1} \end{pmatrix}\begin{pmatrix} a & 1 \\ 1-a^2 & -a \end{pmatrix}\begin{pmatrix} 1 & 0 \\ 0 & b \end{pmatrix}.$$

因 K 的特征数 $\neq 2$, 故 $\begin{pmatrix} 1 & 1 \\ 1-a & -1-a \end{pmatrix}$ 可逆, 所以

$$M=\begin{pmatrix} 1 & 0 \\ 0 & b^{-1} \end{pmatrix}\begin{pmatrix} 1 & 1 \\ 1-a & -1-a \end{pmatrix}\begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$$

$$\cdot\begin{pmatrix} 1 & 1 \\ 1-a & -1-a \end{pmatrix}^{-1}\begin{pmatrix} 1 & 0 \\ 0 & b^{-1} \end{pmatrix}^{-1}.$$

(iii) $b=0$ 而 $c\neq 0$. 由于

$$\begin{pmatrix} a & 0 \\ c & d \end{pmatrix}=\begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}^{-1}\begin{pmatrix} d & -c \\ 0 & a \end{pmatrix}\begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix},$$

所以这个情形可以化到情形 (ii) 去. 至此引理证毕.

现在让我们来证明定理 1. 设 M 表具有固定点 a 和 b 的第一种射影对合的一个矩阵, 则有 K 的中心元素 λ 存在, 使得

$$\lambda M=\begin{pmatrix} 1 & 1 \\ -b & -a \end{pmatrix}\begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}\begin{pmatrix} 1 & 0 \\ -b & -a \end{pmatrix}^{-1},$$

则 $(\lambda M)^2=I$. 反之, 设 M 为非中心矩阵且合于

$$(\lambda M)^2=I,$$

而 λ 为中心元素, 则依引理就有 P 使

$$\lambda M=P^{-1}\begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}P,$$

因 $\begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$ 为第一种射影对合, 所以 M 亦然. 定理证毕.

定理 2　任意两个相异的互相交换的第一种射影对合, 在相似变换之下可以同时化到具有矩阵 $\begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$ 和 $\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$ 的变换

$$x=-y \quad 和 \quad x=y^{-1}.$$

【证】 设 A, B 为两个相异的互相交换的第一种射影对合, 适当选取变换矩阵 A 和 B 的系数后, 我们可以假定

$$A^2 = I, \quad B^2 = I, \quad AB = \lambda BA,$$

而 λ 为中心元素. 不失普遍性, 可以假定

$$A = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}.$$

由

$$B = A^2B = \lambda ABA = \lambda^2 BA^2 = \lambda^2 B,$$

可以推出 $\lambda^2 = 1$, 因而 $\lambda = \pm 1$. 如果 $\lambda = 1$, 则 $AB = BA$, 于是 $B = \begin{pmatrix} b_1 & 0 \\ 0 & b_2 \end{pmatrix}$, 因而 $b_1^2 = b_2^2 = 1$, 那么 A 和 B 表同一射影对合, 此为不可能, 因此 $\lambda = -1$. 由 $AB = -BA$ 可以推出 $B = \begin{pmatrix} 0 & b_1 \\ b_2 & 0 \end{pmatrix}$, 于是 $B = \begin{pmatrix} 0 & b \\ b^{-1} & 0 \end{pmatrix}$. 因为

$$\begin{pmatrix} 1 & 0 \\ 0 & b^{-1} \end{pmatrix}^{-1} \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix} \begin{pmatrix} 1 & 0 \\ 0 & b^{-1} \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix},$$

$$\begin{pmatrix} 1 & 0 \\ 0 & b^{-1} \end{pmatrix}^{-1} \begin{pmatrix} 0 & b \\ b^{-1} & 0 \end{pmatrix} \begin{pmatrix} 1 & 0 \\ 0 & b^{-1} \end{pmatrix} = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix},$$

所以 A 和 B 同时化到了定理所要求的形状.

定理 3 两个第一种射影对合相交换当且仅当它们的固定点组成一个调和点列.

【证】 根据定理 2, 两个相交换的第一种射影对合在相似变换之下, 可以同时化到 $\begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$ 和 $\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$. 可是 $\begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$ 和 $\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$ 的固定点 $0, \infty$ 和 $1, -1$ 组成调和点列, 因之原来的四个点也成调和点列.

反之, 设两个第一种射影对合的固定点组成调和点列. 这四个点在射影变换之下, 可以变到 $0, \infty, 1, -1$, 因之, 在此射影变换之下, 这两个射影对合就变到了 $\begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$ 和 $\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$. 因为射影对合 $\begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$ 和 $\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$ 可交换, 所以原来的两个也可交换.

定理 4 设 $x^2 = -1$ 在体中无解, 则只有两个互相交换的第一种射影对合. 否则, 互相交换的第一种射影对合的个数会大于 2.

【证】 射影对合 $\begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$ 和 $\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$ 互相交换. 假定有两个以上互相交换的射影对合, 依定理 2, 可以假定其中的两个同时变到了 $\begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$ 和 $\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$. 设第三个射影对合为 C, 我们可以假定 $C^2 = I$, 因为

$$C\begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix} = -\begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}C,$$

所以

$$C = \begin{pmatrix} 0 & a \\ a^{-1} & 0 \end{pmatrix}.$$

可是由

$$\begin{pmatrix} 0 & a \\ a^{-1} & 0 \end{pmatrix}\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} = -\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}\begin{pmatrix} 0 & a \\ a^{-1} & 0 \end{pmatrix},$$

又推出 $a = -a^{-1}$, 因此 $a^2 = -1$, 这是不可能的, 除非 $x^2 = -1$ 在体中有解.

定理 5 除了含四元数体作为子体的那些体以外, 我们顶多有三个互相交换的第一种射影对合. 而对于含有四元数体作为子体的体, 我们恰有五个互相交换的第一种射影对合.

【证】 如果方程 $x^2 = -1$ 在体中不可解, 则依定理 4 有且仅有两个互相交换的第一种射影对合. 如果 $x^2 = -1$ 在体中有解, 以 i 表它的一个解, 则依定理 4 的证明, 我们有三个互相交换的第一种射影对合:

$$\begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}, \quad \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}, \quad \begin{pmatrix} 0 & i \\ -i & 0 \end{pmatrix}.$$

如果还有第四个与上面三个互相交换的射影对合, 则依定理 4 的证明, 它一定具有形状

$$\begin{pmatrix} 0 & a \\ a^{-1} & 0 \end{pmatrix},$$

而 $a^2 = -1$(因而 $a^{-1} = -a$). 由

$$\begin{pmatrix} 0 & i \\ -i & 0 \end{pmatrix}\begin{pmatrix} 0 & a \\ -a & 0 \end{pmatrix} = -\begin{pmatrix} 0 & a \\ -a & 0 \end{pmatrix}\begin{pmatrix} 0 & i \\ -i & 0 \end{pmatrix}$$

可以推出 $ia = -ai$.

现在假定有一组互相交换的第一种射影对合:

$$\begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}, \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}, \cdots, \begin{pmatrix} 0 & a_r \\ -a_r & 0 \end{pmatrix}, \cdots,$$

则

(6) $$a_r a_s + a_s a_r = 0 \quad (r \neq s),$$

$$a_r^2 = -1.$$

因为当 $r \geqslant 3$ 时,

$$\begin{aligned} &(a_1a_2 - a_r)(a_2a_1 - a_r) \\ =& a_1a_2^2a_1 - a_ra_2a_1 - a_1a_2a_r + a_r^2 \\ =& 1 + a_1a_2a_r - a_1a_2a_r - 1 = 0, \end{aligned}$$

所以我们一定有 $a_r = a_1a_2$ 或 $a_r = a_2a_1$, 但 $a_1a_2 + a_2a_1 = 0$, 因此方程 (6) 除去一个乘积常数之外, 只有一个或三个解. 如果 (6) 只有一个解, 则我们有三个互相交换的第一种射影对合:

$$\begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}, \quad \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}, \quad \begin{pmatrix} 0 & i \\ -i & 0 \end{pmatrix}.$$

如果 (6) 有三个解 i, j, k, 则我们就有五个互相交换的第一种射影对合:

$$\begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}, \quad \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}, \quad \begin{pmatrix} 0 & i \\ -i & 0 \end{pmatrix}, \quad \begin{pmatrix} 0 & j \\ -j & 0 \end{pmatrix}, \quad \begin{pmatrix} 0 & k \\ -k & 0 \end{pmatrix}.$$

这时如果把关于中心线性无关的元素 i, j, k 添加到体之中心上去, 我们就得到一个四元数体. 反之, 如果我们的体包有四元数体作为子体, 我们确有五个互相交换的第一种射影对合. 定理证毕.

定义 2 两个互相交换的第一种射影对合之积称为第二种射影对合.

与定理 1 平行, 我们可以证明

定理 6 一个非中心矩阵 M 表一个第二种射影对合的充要条件为有一个中心元素 λ 存在, 使得

$$(\lambda M)^2 = -I.$$

如同定理 1 一样, 这个定理有赖于

引理 2 设 M 为非中心的可逆矩阵, 则 $M^2 = -I$ 成立当且仅当有一个可逆矩阵 P 存在, 使得

$$M = P^{-1} \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix} P.$$

【证】 设 $M = P^{-1}\begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}P$, 则 $M^2 = P^{-1}\begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}\begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}P = -I$. 反之, 设 $M^2 = -I$. 将 M 写作 $M = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$, 则由 $M^2 = -I$ 可以得出

$$(7)\qquad \begin{cases} a^2 + bc = cb + d^2 = -1, \\ ab + bd = ca + dc = 0. \end{cases}$$

我们分下面三种情形来研究:

(i) $b \neq 0$. 由 (7) 中解出 c 和 d, 有

$$c = b^{-1}(-1 - a^2), \quad d = -b^{-1}ab.$$

于是

$$\begin{aligned} M &= \begin{pmatrix} a & b \\ b^{-1}(-1 - a^2) & -b^{-1}ab \end{pmatrix} \\ &= \begin{pmatrix} 1 & 0 \\ 0 & b^{-1} \end{pmatrix}\begin{pmatrix} a & 1 \\ -1 - a^2 & -a \end{pmatrix}\begin{pmatrix} 1 & 0 \\ 0 & b \end{pmatrix} \\ &= \begin{pmatrix} 1 & 0 \\ 0 & b^{-1} \end{pmatrix}\begin{pmatrix} 0 & -1 \\ 1 & a \end{pmatrix}\begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}\begin{pmatrix} a & 1 \\ -1 & 0 \end{pmatrix}\begin{pmatrix} 1 & 0 \\ 0 & b \end{pmatrix}. \end{aligned}$$

(ii) $b = 0$ 而 $c \neq 0$. 因为

$$\begin{pmatrix} a & 0 \\ c & d \end{pmatrix} = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}^{-1}\begin{pmatrix} d & -c \\ 0 & a \end{pmatrix}\begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix},$$

所以这个情形可以化到 (i) 去.

(iii) $b = c = 0$. 这时 $a^2 = d^2 = -1$. 如果 $a \neq d$, 则 $a - d \neq 0$. 所以

$$\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}^{-1}\begin{pmatrix} a & 0 \\ 0 & d \end{pmatrix}\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} a & a - d \\ 0 & d \end{pmatrix},$$

因而也可以化到 (i) 去.

现在我们来证明定理 6. 设 M 表第二种射影对合, 则有一中心元素 λ 存在, 使得 $\lambda M = AB$, 而有 $A^2 = B^2 = I, AB = -BA$. 因此

$$(\lambda M)^2 = ABAB = -BAAB = -I.$$

反之, 设 M 为非中心矩阵而具有性质 $(\lambda M)^2=-I$, 依引理 2 就有

$$\lambda M=P^{-1}\begin{pmatrix}0&1\\-1&0\end{pmatrix}P.$$

可是

$$\begin{pmatrix}0&1\\-1&0\end{pmatrix}=\begin{pmatrix}1&0\\0&-1\end{pmatrix}\begin{pmatrix}0&1\\1&0\end{pmatrix},$$

所以

$$\lambda M=\left[P^{-1}\begin{pmatrix}1&0\\0&-1\end{pmatrix}P\right]\left[P^{-1}\begin{pmatrix}0&1\\1&0\end{pmatrix}P\right]$$

是两个互相交换的第一种射影对合之积.

【备注 1】　如果 $x^2=-1$ 在中心中可解, 则第二种射影对合就是第一种射影对合, 反之亦然. 因为如果 $M^2=-I$, 设 λ 为 $x^2=-1$ 的一解, 则 $(\lambda M)^2=I$, 而如果 $M^2=I$, 则 $(\lambda M)^2=-I$.

【备注 2】　周期 2 的矩阵不全是射影对合. 例如, 如果 K 是有理数域, 则 $\begin{pmatrix}0&1\\\rho&0\end{pmatrix}$ 的周期是 2, 可是它不是射影对合.

§4　体上的二级线性群

设 K 为体, 它的特征数任意. 以 K^* 表 K 的乘法群, K 上所有 2×2 可逆矩阵组成一群, 记作 $GL_2(K)$, 称为 K 上二级一般线性群. 显然以下这些元素属于 $GL_2(K)$:

(1)
$$T_{12}(\lambda)=\begin{pmatrix}1&\lambda\\0&1\end{pmatrix},\quad T_{21}(\mu)=\begin{pmatrix}1&0\\\mu&1\end{pmatrix},$$

其中 $\lambda,\mu\in K^*$. 以 $SL_2(K)$ 表由一切 $T_{12}(\lambda)$ 及 $T_{21}(\mu)(\lambda,\mu$ 跑过 $K^*)$ 所生成的群, 显然 $SL_2(K)$ 是 $GL_2(K)$ 的子群. 我们把 $SL_2(K)$ 称为 K 上二级特殊线性群.

注意以下这些元素都属于 $SL_2(K)$:

(2)
$$\begin{pmatrix}0&1\\-1&0\end{pmatrix}=\begin{pmatrix}1&0\\-1&1\end{pmatrix}\begin{pmatrix}1&1\\0&1\end{pmatrix}\begin{pmatrix}1&0\\-1&1\end{pmatrix},$$

(3)
$$\begin{pmatrix}\lambda&0\\0&\lambda^{-1}\end{pmatrix}=\begin{pmatrix}1&-\lambda\\0&1\end{pmatrix}\begin{pmatrix}1&0\\\lambda^{-1}&1\end{pmatrix}\begin{pmatrix}0&1\\-1&0\end{pmatrix}\begin{pmatrix}1&0\\\lambda&1\end{pmatrix}$$

及

$$(4)\quad \begin{pmatrix} 1 & 0 \\ 0 & \lambda\mu\lambda^{-1}\mu^{-1} \end{pmatrix} = \begin{pmatrix} \lambda^{-1} & 0 \\ 0 & \lambda \end{pmatrix} \begin{pmatrix} \mu^{-1} & 0 \\ 0 & \mu \end{pmatrix} \begin{pmatrix} \mu\lambda & 0 \\ 0 & (\mu\lambda)^{-1} \end{pmatrix}.$$

首先, 我们来证明

定理 1　$GL_2(K)$ 中每一个元素皆可表成

$$B\begin{pmatrix} 1 & 0 \\ 0 & \lambda \end{pmatrix},$$

其中 $B \in SL_2(K)$ 而 $\lambda \in K^*$.

【证】　设 $A = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in GL_2(K)$. 如果 $a \neq 0$, 则

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ ca^{-1} & 1 \end{pmatrix} \begin{pmatrix} a & b \\ 0 & d - ca^{-1}b \end{pmatrix}$$

$$= \begin{pmatrix} 1 & 0 \\ ca^{-1} & 1 \end{pmatrix} \begin{pmatrix} 1 & b(d - ca^{-1}b)^{-1} \\ 0 & 1 \end{pmatrix} \begin{pmatrix} a & 0 \\ 0 & a^{-1} \end{pmatrix} \begin{pmatrix} 1 & 0 \\ 0 & a(d - ca^{-1}b) \end{pmatrix}.$$

注意, 这里 $d - ca^{-1}b \neq 0$ 一定成立. 在上面的乘积中, 第一个元素是 $T_{21}(ca^{-1})$, 第二个元素是 $T_{12}(b(d - ca^{-1}b)^{-1})$, 而依 (3) 知第三个元素亦属于 $SL_2(K)$. 所以这时本定理成立.

其次, 研究 $a = 0$ 的情形. 因 A 可逆, 这时必有 $c \neq 0$, 于是

$$\begin{pmatrix} 0 & b \\ c & d \end{pmatrix} = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix} \begin{pmatrix} -c & -d \\ 0 & b \end{pmatrix}$$

$$= \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix} \begin{pmatrix} 1 & -db^{-1} \\ 0 & 1 \end{pmatrix} \begin{pmatrix} -c & 0 \\ 0 & -c^{-1} \end{pmatrix} \begin{pmatrix} 1 & 0 \\ 0 & -cb \end{pmatrix}.$$

本定理由 (2), (3) 式推出.

更进一步我们有

定理 2　$SL_2(K)$ 是 $GL_2(K)$ 的正规子群.

【证】　依定理 1, 只要证明 $SL_2(K)$ 的生成元被形如 $\begin{pmatrix} 1 & 0 \\ 0 & a \end{pmatrix}$ $(a \in K^*)$ 的

元素作用后仍变为 $SL_2(K)$ 中的元素即可，而这是很显然的：

$$\begin{pmatrix} 1 & 0 \\ 0 & a \end{pmatrix}\begin{pmatrix} 1 & \lambda \\ 0 & 1 \end{pmatrix}\begin{pmatrix} 1 & 0 \\ 0 & a \end{pmatrix}^{-1} = \begin{pmatrix} 1 & \lambda a^{-1} \\ 0 & 1 \end{pmatrix},$$

$$\begin{pmatrix} 1 & 0 \\ 0 & a \end{pmatrix}\begin{pmatrix} 1 & 0 \\ \mu & 1 \end{pmatrix}\begin{pmatrix} 1 & 0 \\ 0 & a \end{pmatrix}^{-1} = \begin{pmatrix} 1 & 0 \\ a\mu & 1 \end{pmatrix}.$$

定理 3 $SL_2(K)$ 永远包含 $GL_2(K)$ 的换位子群. 更进一步，除开 $K = F_2$ 的情形之外，$SL_2(K)$ 就是 $GL_2(K)$ 的换位子群.

【证】 设 A_1, A_2 为 $GL_2(K)$ 中任意二元素. 依定理 1，可以写

$$A_1 = B_1\begin{pmatrix} 1 & 0 \\ 0 & \lambda_1 \end{pmatrix}, \quad A_2 = B_2\begin{pmatrix} 1 & 0 \\ 0 & \lambda_2 \end{pmatrix},$$

其中 $B_1, B_2 \in SL_2(K), \lambda_1, \lambda_2 \in K^*$. 因 $SL_2(K)$ 是 $GL_2(K)$ 的正规子群，故有

$$\begin{aligned} & A_1A_2A_1^{-1}A_2^{-1}SL_2(K) \\ = & \begin{pmatrix} 1 & 0 \\ 0 & \lambda_1 \end{pmatrix}\begin{pmatrix} 1 & 0 \\ 0 & \lambda_2 \end{pmatrix}\begin{pmatrix} 1 & 0 \\ 0 & \lambda_1^{-1} \end{pmatrix}\begin{pmatrix} 1 & 0 \\ 0 & \lambda_2^{-1} \end{pmatrix}SL_2(K) \\ = & \begin{pmatrix} 1 & 0 \\ 0 & \lambda_1\lambda_2\lambda_1^{-1}\lambda_2^{-1} \end{pmatrix}SL_2(K). \end{aligned}$$

依 (4) 式知

$$\begin{pmatrix} 1 & 0 \\ 0 & \lambda_1\lambda_2\lambda_1^{-1}\lambda_2^{-1} \end{pmatrix} \in SL_2(K),$$

故

$$A_1A_2A_1^{-1}A_2^{-1} \in SL_2(K).$$

这就证明了 $SL_2(K)$ 永远包含 $GL_2(K)$ 的换位子群.

现在，我们来证明，除开 $K = F_2$ 这一情形外，$SL_2(K)$ 一定包含在 $GL_2(K)$ 的换位子群里. 以 $\mathfrak{C}$ 表 $GL_2(K)$ 的换位子群. 我们先来证明，如 $\mathfrak{C}$ 包有一个 $T_{12}(\lambda_0)$ $(\lambda_0 \in K^*)$，则 $\mathfrak{C} \supseteq SL_2(K)$. 实际上，如 $\mathfrak{C}$ 包有 $T_{12}(\lambda_0)$，则 $\mathfrak{C}$ 包有

$$\begin{pmatrix} 1 & 0 \\ 0 & \mu \end{pmatrix}T_{12}(\lambda_0)\begin{pmatrix} 1 & 0 \\ 0 & \mu \end{pmatrix}^{-1} = T_{12}(\lambda_0\mu^{-1}).$$

当 μ 跑过 K^* 时，$\lambda_0\mu^{-1}$ 亦然. 因此 $\mathfrak{C}$ 包有一切 $T_{12}(\lambda)$ $(\lambda \in K^*)$. 其次，因

$$T_{21}(\lambda) = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}T_{12}(-\lambda)\begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}^{-1},$$

故 $\mathfrak{C}$ 亦包有一切 $T_{21}(\lambda)$ $(\lambda \in K^*)$. 所以 $\mathfrak{C} \supseteq SL_2(K)$.

其次, 我们证明, 如 $K \neq F_2$, 则 $\mathfrak{C}$ 包有某一个 $T_{12}(\lambda)$. 注意, $\mathfrak{C}$ 包有

$$\begin{pmatrix} 1 & 0 \\ 0 & \lambda \end{pmatrix}^{-1} \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}^{-1} \begin{pmatrix} 1 & 0 \\ 0 & \lambda \end{pmatrix} \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} 1 & 1-\lambda \\ 0 & 1 \end{pmatrix},$$

因为 $K \neq F_2$, 所以有 $\lambda \in K^*$, 使 $1-\lambda \neq 0$. 因此断言成立.

综合以上讨论, 我们就得出, 当 $K \neq F_2$ 时, $SL_2(K)$ 就是 $GL_2(K)$ 的换位子群.

当 $K = F_2$ 时, 我们有

$$\begin{aligned} GL_2(K) = &\left\{ \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix}, \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}, \begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix}, \begin{pmatrix} 0 & 1 \\ 1 & 1 \end{pmatrix} \right\} \\ = &SL_2(K). \end{aligned}$$

易证, 这时 $GL_2(K) \cong \mathfrak{S}_3$(三个文字的对称群). 我们知道 $\mathfrak{S}_3$ 的换位子群是三个文字的交错群 $\mathscr{A}_3$, 因此这时 $SL_2(K) \neq GL_2(K)$ 的换位子群.

现在我们来研究 $GL_2(K)/SL_2(K)$ 的构造. 我们有

定理 4　$GL_2(K)/SL_2(K) \cong K^*/C$, 其中 C 表 K^* 之换位子群.

【证】　以 $\lambda \to \varphi(\lambda)$ 表从 K^* 到 Abel 群 K^*/C 的自然同态. 设 $\begin{pmatrix} a & b \\ c & d \end{pmatrix} \in GL_2(K)$, 以 $\begin{pmatrix} a' & b' \\ c' & d' \end{pmatrix}$ 表其逆. 定义

$$\Delta \begin{pmatrix} a & b \\ c & d \end{pmatrix} = \begin{cases} \varphi(ad'^{-1}) & 若 d' \neq 0, \\ \varphi(-bb'^{-1}) & 若 b' \neq 0, \\ \varphi(-cc'^{-1}) & 若 c' \neq 0, \\ \varphi(da'^{-1}) & 若 a' \neq 0, \end{cases}$$

则

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} \to \Delta \begin{pmatrix} a & b \\ c & d \end{pmatrix}$$

是从 $GL_2(K)$ 到 K^*/C 之中的一个映射. 我们要证明这个映射是单值的、映上的同态映射.

I. Δ 的单值性. 我们有

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} \begin{pmatrix} a' & b' \\ c' & d' \end{pmatrix} = \begin{pmatrix} a' & b' \\ c' & d' \end{pmatrix} \begin{pmatrix} a & b \\ c & d \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}. \tag{5}$$

利用此式即可算出, 当 a',b',c',d' 均不为 0 时,

$$\begin{aligned}\varphi(ad'^{-1}) &= \varphi(-bd'b'^{-1}d'^{-1}) = \varphi(-bb'^{-1})\\ &= \varphi(a'^{-1}b'db'^{-1}) = \varphi(da'^{-1})\\ &= \varphi(-ca'c'^{-1}a'^{-1}) = \varphi(-cc'^{-1}).\end{aligned}$$

当 a',b',c',d' 中有等于 0 的时候, 亦可同样进行计算. 这就证明 Δ 是单值的.

II. Δ 是映上的. 易见

$$\Delta\begin{pmatrix}1 & 0\\ 0 & \lambda\end{pmatrix} = \varphi(\lambda),$$

对一切 $\lambda\in K^*$. 因而 Δ 是映上的.

III. Δ 是同态. 首先指出一个恒等式: 当 $\lambda,\mu\in K^*$ 而 $\lambda\neq-\mu^{-1}$ 时,

$$(1+\lambda\mu)(1+\mu\lambda)^{-1} = \lambda(\lambda^{-1}+\mu)\lambda^{-1}(\lambda^{-1}+\mu)^{-1}. \tag{6}$$

设 $\begin{pmatrix}a & b\\ c & d\end{pmatrix}, \begin{pmatrix}a_1 & b_1\\ c_1 & d_1\end{pmatrix}\in GL_2(K)$ 而以 $\begin{pmatrix}a' & b'\\ c' & d'\end{pmatrix}, \begin{pmatrix}a_1' & b_1'\\ c_1' & d_1'\end{pmatrix}$ 分别表它们的逆, 则当 $c_1'b'+d_1'd', a, a_1, d', d_1'$ 都不等于 0 时, 有

$$\begin{aligned}\Delta\left[\begin{pmatrix}a & b\\ c & d\end{pmatrix}\begin{pmatrix}a_1 & b_1\\ c_1 & d_1\end{pmatrix}\right] &= \varphi((aa_1+bc_1)(c_1'b'+d_1'd')^{-1})\\ &= \varphi(aa_1d'^{-1}d_1'^{-1})\varphi((1+a^{-1}bc_1a_1^{-1})(1+d_1'^{-1}c_1'b'd'^{-1})^{-1})\\ &= \varphi(aa_1d'^{-1}d_1'^{-1})\varphi((1+a^{-1}bc_1a_1^{-1})(1+c_1a_1^{-1}a^{-1}b)^{-1})\\ &= \varphi(ad'^{-1})\varphi(a_1d_1'^{-1}) = \Delta\begin{pmatrix}a & b\\ c & d\end{pmatrix}\Delta\begin{pmatrix}a_1 & b_1\\ c_1 & d_1\end{pmatrix}.\end{aligned}$$

其余情形亦可类似地加以计算.

最后我们来证明 Δ 的核即为 $SL_2(K)$, 这样, 本定理即由同态基本定理推出. 首先, 显然有

$$\Delta\begin{pmatrix}1 & \lambda\\ 0 & 1\end{pmatrix} = C,\quad \Delta\begin{pmatrix}1 & 0\\ \mu & 1\end{pmatrix} = C,$$

因此 $SL_2(K)$ 包在 Δ 的核之中. 其次, 设 $A\in GL_2(K)$, 将 A 写作

$$A = B\begin{pmatrix}1 & 0\\ 0 & \lambda\end{pmatrix},$$

则

$$\Delta(A) = \varphi(\lambda).$$

因此 $\Delta(A) = C$ 当且仅当 $\lambda \in C$. 由 (4) 式知, 当 $\lambda \in C$ 时,

$$\begin{pmatrix} 1 & 0 \\ 0 & \lambda \end{pmatrix} \in SL_2(K).$$

这就证明了 Δ 的核即为 $SL_2(K)$. 本定理至此完全证毕.

在证明定理 4 的过程中, 我们还证明了

系理　元素 $\begin{pmatrix} 1 & 0 \\ 0 & \lambda \end{pmatrix}$ 属于 $SL_2(K)$ 当且仅当 $\lambda \in C$.

在证明定理 4 的过程中所引进的 $\Delta \begin{pmatrix} a & b \\ c & d \end{pmatrix}$, 我们称之为可逆矩阵的行列式. 易见, 当 K 为域时, 这就是通常的行列式, $\Delta \begin{pmatrix} a & b \\ c & d \end{pmatrix}$ 是 K^* 中的元素. 但需注意, 当 K 不是域时, $\Delta \begin{pmatrix} a & b \\ c & d \end{pmatrix}$ 是 K^*/C 中的元素, 而不是 K^* 中的元素.

现在我们来确定 $GL_2(K)$ 及 $SL_2(K)$ 的中心. 以 Z 表 K 的中心, 以 Z_2 表 $GL_2(K)$ 的中心, 我们有

定理 5　Z_2 由一切矩阵 $\lambda I(\lambda \in Z^*)$ 所组成, 而 $SL_2(K)$ 的中心即 $Z_2 \cap SL_2(K)$.

【证】　易见 $\lambda I(\lambda \in Z^*)$ 是 $GL_2(K)$ 的中心元素. 反之, 设 $A = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$ 为 $GL_2(K)$ 的中心元素, 则由

$$\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}\begin{pmatrix} a & b \\ c & d \end{pmatrix} = \begin{pmatrix} a & b \\ c & d \end{pmatrix}\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$$

及

$$\begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix}\begin{pmatrix} a & b \\ c & d \end{pmatrix} = \begin{pmatrix} a & b \\ c & d \end{pmatrix}\begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix}$$

推出 $b = c = 0$ 及 $a = d$, 再由

$$\begin{pmatrix} 1 & \mu \\ 0 & 1 \end{pmatrix}\begin{pmatrix} a & 0 \\ 0 & a \end{pmatrix} = \begin{pmatrix} a & 0 \\ 0 & a \end{pmatrix}\begin{pmatrix} 1 & \mu \\ 0 & 1 \end{pmatrix}$$

对一切 $\mu \in K$ 推出 $a \in Z^*$. 因此, Z_2 由一切矩阵 $\lambda I(\lambda \in Z^*)$ 所组成.

因为 $\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$, $\begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix}$, $\begin{pmatrix} 1 & \mu \\ 0 & 1 \end{pmatrix}$ 皆 $SL_2(K)$ 中的元素, 在上面的证明过程中, 实际上也证明了 $SL_2(K)$ 的中心即为 $Z_2 \cap SL_2(K)$. 本定理证毕.

我们也把 $GL_2(K)/Z_2$ 称为 K 上二级射影一般线性群, 并已证明它同构于 $PGL_2(K)$. 现在我们再把 $SL_2(K)/(Z_2 \cap SL_2(K))$ 称为 K 上二级射影特殊线性群,

并记作 $PSL_2(K)$. 显然 $PSL_2(K)$ 与 $SL_2(K)$ 在自然同态 $GL_2(K)\to PGL_2(K)$ 之下的像同构. 而且, 除开 $K=F_2$ 以外, $PSL_2(K)$ 即是 $PGL_2(K)$ 的换位子群.

定义 设 $M(\neq I)\in GL_2(K)$. 如果 $M^2=I$, 则 M 称为对合, 它们的全体生成一群, 记作 $SL_2^{\pm}(K)$. $SL_2^{\pm}(K)$ 对其中心的商群记作 $PSL_2^{\pm}(K)$.

定理 6 当 K 的特征数 =2 或当 K 的特征数 $\neq 2$ 而 $-1\in C$ 时, $SL_2^{\pm}(K)=SL_2(K)$. 否则, $SL_2^{\pm}(K)$ 可从 $SL_2(K)$ 添加一个对合而得到.

【证】 当 K 的特征数 =2 时, $T_{12}(\lambda)$ 及 $T_{21}(\mu)$ 皆对合, 因此 $SL_2(K)\subseteq SL_2^{\pm}(K)$. 反之, 设 $M=\begin{pmatrix} a & b\\ c & d\end{pmatrix}$ 为一个对合. 先设 $a=0$, 则由 $\begin{pmatrix} 0 & b\\ c & d\end{pmatrix}^2=\begin{pmatrix} 1 & 0\\ 0 & 1\end{pmatrix}$ 推出 $c=b^{-1}$ 及 $d=0$. 于是

$$\begin{pmatrix} 0 & b\\ b^{-1} & 0\end{pmatrix}=\begin{pmatrix} b & 0\\ 0 & b^{-1}\end{pmatrix}\begin{pmatrix} 0 & 1\\ 1 & 0\end{pmatrix}\in SL_2(K).$$

再设 $a\neq 0$, 而 $c\neq 0$, 则

$$M_1=\begin{pmatrix} 1 & \lambda\\ 0 & 1\end{pmatrix}\begin{pmatrix} a & b\\ c & d\end{pmatrix}\begin{pmatrix} 1 & \lambda\\ 0 & 1\end{pmatrix}^{-1}=\begin{pmatrix} a+\lambda c & *\\ * & *\end{pmatrix}$$

亦是对合. 可以选取 $\lambda\in K$ 使 $a+\lambda c=0$. 根据上面的证明知 $M_1\in SL_2(K)$, 因 $SL_2(K)$ 为正规子群, 故 $M\in SL_2(K)$. 如果 $a\neq 0$ 而 $c=0$, 则由 $\begin{pmatrix} a & b\\ 0 & d\end{pmatrix}^2=\begin{pmatrix} 1 & 0\\ 0 & 1\end{pmatrix}$ 推出 $a=d=1$, 因之

$$M=T_{12}(b)\in SL_2(K).$$

因此 $SL_2^{\pm}(K)=SL_2(K)$.

其次研究 K 的特征数 $\neq 2$ 的情形. 因

$$\begin{pmatrix} 1 & \lambda\\ 0 & 1\end{pmatrix}=\begin{pmatrix} 1 & 0\\ 0 & -1\end{pmatrix}\begin{pmatrix} 1 & \lambda\\ 0 & -1\end{pmatrix}$$

及

$$\begin{pmatrix} 1 & 0\\ \mu & 1\end{pmatrix}=\begin{pmatrix} 1 & 0\\ 0 & -1\end{pmatrix}\begin{pmatrix} 1 & 0\\ -\mu & -1\end{pmatrix},$$

故 $SL_2(K) \subseteq SL_2^{\pm}(K)$. 其次, 设 M 为一个对合, 依引理 3.2, 可将 M 表成 $P\begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}P^{-1}(P \in GL_2(K))$. 如 $-1 \in C$, 依定理 4 的系理, $\begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix} \in SL_2(K)$, 因之 $M \in SL_2(K)$, 故 $SL_2^{\pm}(K) = SL_2(K)$.

最后, 如 K 的特征数 $\neq 2$ 而 $-1 \notin C$, 则将 M 添加到 $SL_2(K)$ 之后,

$$M\begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}\begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix} = P\begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}P^{-1}\begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}^{-1}\begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$$

亦添到 $SL_2(K)$ 之中, 因之 $\begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$ 就添到里面. 因此所有对合就都添到里面.

本定理至此完全证毕.

显而易见 $SL_2^{\pm}(K)$ 的中心为 $Z_2 \cap SL_2^{\pm}(K)$. 于是有

$$PSL_2^{\pm}(K) = SL_2^{\pm}(K)/(Z_2 \cap SL_2^{\pm}(K)).$$

我们同样知道 $PSL_2^{\pm}(K)$ 与 $SL_2^{\pm}(K)$ 在自然同态 $GL_2(K) \to PGL_2(K)$ 之下的像同构.

§5 $PSL_2(K)$ 的单性

在本节中我们将证明, 除开 $K = F_2$ 及 F_3 这两个情形之外, $PSL_2(K)$ 是单群. 为此我们先证次之引理.

引理 1 设 $\mathfrak{N}$ 是 $GL_2(K)$ 的一个子群, 并假定它在 $SL_2(K)$ 之下不变, 即 $B\mathfrak{N}B^{-1} \subseteq \mathfrak{N}$, 对一切 $B \in SL_2(K)$. 如果 $\mathfrak{N}$ 包有 $T_{12}(1)$, 则 $\mathfrak{N} \supseteq SL_2(K)$.

【证】 设 $\mathfrak{N}$ 包有 $T_{12}(1)$. 因 $\mathfrak{N}$ 在 $SL_2(K)$ 之下不变, 故 $\mathfrak{N}$ 亦包有

$$(1) \qquad \begin{pmatrix} \lambda & 0 \\ 0 & \lambda^{-1} \end{pmatrix}\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}\begin{pmatrix} \lambda & 0 \\ 0 & \lambda^{-1} \end{pmatrix}^{-1} = \begin{pmatrix} 1 & \lambda^2 \\ 0 & 1 \end{pmatrix},$$

对一切 $\lambda \in K^*$. 于是 $\mathfrak{N}$ 包有

$$(2) \qquad \begin{pmatrix} 1(\lambda+1)^2 \\ 1 \end{pmatrix}\begin{pmatrix} 1 & \lambda^2 \\ 0 & 1 \end{pmatrix}^{-1}\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}^{-1} = \begin{pmatrix} 1 & 2\lambda \\ 0 & 1 \end{pmatrix},$$

对一切 $\lambda \in K^*$.

如 K 的特征数 $\neq 2$, 则当 λ 跑过 K^* 时, 2λ 亦跑过 K^*, 因此 $\mathfrak{N}$ 包有一切 $T_{12}(\lambda)(\lambda \in K^*)$. 又因为

$$\begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}\begin{pmatrix} 1 & -\mu \\ 0 & 1 \end{pmatrix}\begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}^{-1} = \begin{pmatrix} 1 & 0 \\ \mu & 1 \end{pmatrix},$$

故 $\mathfrak{N}$ 亦包有一切 $T_{21}(\mu)(\mu \in K^*)$. 因此 $\mathfrak{N} \supseteq SL_2(K)$.

其次, 设 K 的特征数 =2. 我们已经知道 $\mathfrak{N}$ 包有

$$\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} \quad 及 \quad \begin{pmatrix} 0 & \lambda^2 \\ 0 & 1 \end{pmatrix},$$

对一切 $\lambda \in K^*$. 因

$$\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}^{-1} = \begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix},$$

故 $\mathfrak{N}$ 亦包有 $T_{21}(1)$. 于是 $\mathfrak{N}$ 亦包有

$$\begin{pmatrix} \lambda^{-1} & 0 \\ 0 & \lambda \end{pmatrix}\begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix}\begin{pmatrix} \lambda^{-1} & 0 \\ 0 & \lambda \end{pmatrix}^{-1} = \begin{pmatrix} 1 & 0 \\ \lambda^2 & 1 \end{pmatrix},$$

对一切 $\lambda \in K^*$. 因之 $\mathfrak{N}$ 亦包有

$$\begin{pmatrix} 1 & \lambda^2 \\ 0 & 1 \end{pmatrix}\begin{pmatrix} 1 & 0 \\ \lambda^{-2} & 1 \end{pmatrix}\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}\begin{pmatrix} 1 & 0 \\ \lambda^2 & 1 \end{pmatrix} = \begin{pmatrix} \lambda^2 & 0 \\ 0 & \lambda^{-2} \end{pmatrix},$$

对一切 $\lambda \in K^*$. 于是从

$$\begin{pmatrix} 1 & \lambda \\ 0 & 1 \end{pmatrix}\begin{pmatrix} \lambda^2 & 0 \\ 0 & \lambda^{-2} \end{pmatrix}\begin{pmatrix} 1 & \lambda \\ 0 & 1 \end{pmatrix}^{-1}\begin{pmatrix} \lambda^2 & 0 \\ 0 & \lambda^2 \end{pmatrix}^{-1} = \begin{pmatrix} 1 & 1+\lambda^5 \\ 0 & 1 \end{pmatrix},$$

推出 $\mathfrak{N}$ 包有 $T_{12}(\lambda+\lambda^5)$, 对一切 $\lambda \in K^*$. 可是,

$$\begin{pmatrix} (\lambda+1)^2 & 0 \\ 0 & (\lambda+1)^{-2} \end{pmatrix}^{-1}\begin{pmatrix} 1 & \lambda+\lambda^5 \\ 0 & 1 \end{pmatrix}\begin{pmatrix} (\lambda+1)^2 & 0 \\ 0 & (\lambda+1)^{-2} \end{pmatrix} = \begin{pmatrix} 1 & \lambda \\ 0 & 1 \end{pmatrix},$$

对一切 $\lambda \in K^*$ 而 $\lambda \neq 1$, 因此 $\mathfrak{N}$ 包有 $T_{12}(\lambda)(\lambda \in K^*)$ 而 $\lambda \neq 1$. 我们已经假设 $\mathfrak{N}$ 包有 $T_{12}(1)$, 因此 $\mathfrak{N}$ 包有 $T_{12}(\lambda)$, 对一切 $\lambda \in K^*$. 像前一情形一样, 可以推出 $\mathfrak{N} \supseteq SL_2(K)$.

引理 2 设 $\mathfrak{N}$ 是 $GL_2(K)$ 的一个子群, 如果 $\mathfrak{N}$ 的一个共轭子群包有 $SL_2(K)$, 则 $\mathfrak{N}$ 亦包有 $SL_2(K)$.

【证】 设 $A\mathfrak{N}A^{-1}$ 是 $\mathfrak{N}$ 的一个共轭子群, $A \in GL_2(K)$. 假设

$$A\mathfrak{N}A^{-1} \supseteq SL_2(K),$$

则

$$\mathfrak{N} \supseteq A^{-1}SL_2(K)A = SL_2(K).$$

基于引理 1 及引理 2 可推出

引理 3　设 $\mathfrak{N}$ 是 $GL_2(K)$ 的一个子群, 并假定它在 $SL_2(K)$ 之下不变. 如果 $\mathfrak{N}$ 包有一个 $T_{12}(\lambda_0)(\lambda_0 \in K^*)$, 则 $\mathfrak{N} \supseteq SL_2(K)$.

【证】　设 $\mathfrak{N}$ 包有 $T_{12}(\lambda_0)$. 令 $A = \begin{pmatrix} 1 & 0 \\ 0 & \lambda_0 \end{pmatrix}$, 则 $A\mathfrak{N}A^{-1}$ 包有

$$\begin{pmatrix} 1 & 0 \\ 0 & \lambda_0 \end{pmatrix}\begin{pmatrix} 1 & \lambda_0 \\ 0 & 1 \end{pmatrix}\begin{pmatrix} 1 & 0 \\ 0 & \lambda_0 \end{pmatrix}^{-1} = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}.$$

我们来证明, $A\mathfrak{N}A^{-1}$ 在 $SL_2(K)$ 之下不变. 实际上, 设 $B \in SL_2(K)$, 则 $A^{-1}BA \in SL_2(K)$. 因 $\mathfrak{N}$ 在 $SL_2(K)$ 之下不变,

$$BA\mathfrak{N}A^{-1}B^{-1} = A(A^{-1}BA)\mathfrak{N}(A^{-1}BA)^{-1}A^{-1} = A\mathfrak{N}A^{-1}.$$

依引理 1, $A\mathfrak{N}A^{-1}$ 包有 $SL_2(K)$. 再依引理 2, $\mathfrak{N} \supseteq SL_2(K)$.

现在我们来证明次之定理.

定理 1　设 $K \neq F_2$ 及 F_3, 而 $\mathfrak{N}$ 为 $GL_2(K)$ 的子群, 并假定 $\mathfrak{N}$ 在 $SL_2(K)$ 之下不变. 如果 $\mathfrak{N} \not\subseteq Z_2$, 则 $\mathfrak{N} \supseteq SL_2(K)$,

【证】　证明分三步进行. 首先我们证明, 如果 $\mathfrak{N} \not\subseteq Z_2$, 则 $\mathfrak{N}$ 包有一个形如

$$\begin{pmatrix} 0 & b \\ c & d \end{pmatrix} \tag{3}$$

的元素. 设 $A = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathfrak{N}$, 而且 $A \notin Z_2$, 则 $\mathfrak{N}$ 包有

$$\begin{pmatrix} 1 & 0 \\ \lambda & 1 \end{pmatrix}\begin{pmatrix} a & b \\ c & d \end{pmatrix}\begin{pmatrix} 1 & 0 \\ \lambda & 1 \end{pmatrix}^{-1} = \begin{pmatrix} a - b\lambda & * \\ * & * \end{pmatrix} \tag{4}$$

及

$$\begin{pmatrix} 1 & \lambda \\ 0 & 1 \end{pmatrix}\begin{pmatrix} a & b \\ c & d \end{pmatrix}\begin{pmatrix} 1 & \lambda \\ 0 & 1 \end{pmatrix}^{-1} = \begin{pmatrix} a + \lambda c & * \\ * & * \end{pmatrix} \tag{5}$$

对一切 $\lambda \in K$. 如 $b \neq 0$, 在 (4) 中取 $\lambda = b^{-1}a$ 即可; 如 $c \neq 0$, 在 (5) 中取 $\lambda = -ac^{-1}$ 即可. 如 $b = c = 0$, 则 $\mathfrak{N}$ 包有

$$\begin{pmatrix} 1 & \lambda \\ 0 & 1 \end{pmatrix}\begin{pmatrix} a & 0 \\ 0 & d \end{pmatrix}\begin{pmatrix} 1 & \lambda \\ 0 & 1 \end{pmatrix}^{-1} = \begin{pmatrix} a & \lambda d - a\lambda \\ 0 & d \end{pmatrix},$$

对一切 $\lambda \in K^*$. 如 $\lambda d - a\lambda = 0$, 对一切 $\lambda \in K$, 取 $\lambda = 1$ 即得 $a = d$, 因之 $\lambda a = a\lambda$ 对一切 $\lambda \in K$, 即 $a \in Z^*$; 这与 $A \notin Z_2$ 相矛盾. 因之有 $\lambda \in K$ 使 $\lambda d - a\lambda \neq 0$. 这就化到 $b \neq 0$ 的情形去了. 因此断言得证.

其次, 我们来证明如 $K \neq F_5$, 则 $\mathfrak{N}$ 一定包有一个形如

$$\begin{pmatrix} a & b \\ 0 & d \end{pmatrix}$$

的元素, 其中 $a \neq d$ 或 $a = d \notin Z^*$. 设 $\mathfrak{N}$ 包有 (3), 则 $\mathfrak{N}$ 包有

$$\begin{pmatrix} 0 & b \\ c & d \end{pmatrix}^{-1} \begin{pmatrix} \lambda & 0 \\ 0 & \lambda^{-1} \end{pmatrix}^{-1} \begin{pmatrix} 0 & b \\ c & d \end{pmatrix} \begin{pmatrix} \lambda & 0 \\ 0 & \lambda^{-1} \end{pmatrix} = \begin{pmatrix} c^{-1}\lambda c\lambda & * \\ 0 & b^{-1}\lambda^{-1}b\lambda^{-1} \end{pmatrix}.$$

如 $Z \neq F_2, F_3, F_5$, 选取 $\lambda \in Z^*$ 使 $\lambda^4 \neq 1$, 于是 $\mathfrak{N}$ 包有

$$\begin{pmatrix} \lambda^2 & * \\ 0 & \lambda^{-2} \end{pmatrix},$$

而 $\lambda^2 \neq \lambda^{-2}$. 如 $Z = F_2, F_3$ 或 F_5 而 $K \neq F_5$, 选取 $\lambda \in K$ 而 $\lambda c = c\lambda, \lambda^2 \notin Z$, 则 $\mathfrak{N}$ 包有

$$\begin{pmatrix} \lambda^2 & * \\ 0 & b^{-1}\lambda^{-1}b\lambda^{-1} \end{pmatrix}$$

而 $\lambda^2 \notin Z$. 因此断言得证.

最后, 我们来证明 $\mathfrak{N}$ 一定包有一个 $T_{12}(\lambda_0)(\lambda_0 \in K^*)$.

当 $K \neq F_5$ 时, 可假设 $\mathfrak{N}$ 包有 $\begin{pmatrix} a & b \\ 0 & d \end{pmatrix}$, 其中 $a \neq d$ 或 $a = d \notin Z^*$. 于是 $\mathfrak{N}$ 包有

$$\begin{pmatrix} 1 & \lambda \\ 0 & 1 \end{pmatrix} \begin{pmatrix} a & b \\ 0 & d \end{pmatrix} \begin{pmatrix} 1 & \lambda \\ 0 & 1 \end{pmatrix}^{-1} \begin{pmatrix} a & b \\ 0 & d \end{pmatrix}^{-1} = \begin{pmatrix} 1 & \lambda - a\lambda d^{-1} \\ 0 & 1 \end{pmatrix},$$

对一切 $\lambda \in K$. 因 $a \neq d$ 或 $a = d \notin Z^*$, 故可选取 $\lambda \in K$, 使 $\lambda - a\lambda d^{-1} \neq 0$. 当 $K = F_5$ 时, 依第一段的证明, 可假定 $\mathfrak{N}$ 包有 $\begin{pmatrix} 0 & b \\ c & d \end{pmatrix}$. 可以假定 $c = -b^{-1}$. 否则, $\mathfrak{N}$ 包有

$$\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} \begin{pmatrix} 0 & b \\ c & d \end{pmatrix} \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}^{-1} \begin{pmatrix} 0 & b \\ c & d \end{pmatrix}^{-1},$$

这是一个行列式为 1 的非中心元素, 从这个元素出发, 利用第一段的造法即可得到一个形如 $\begin{pmatrix} 0 & b \\ -b^{-1} & d \end{pmatrix}$ 的元素含在 $\mathfrak{N}$ 中. 不妨假设 $d \neq 0$, 否则 $\mathfrak{N}$ 一定包有

$$\begin{pmatrix} 0 & b \\ -b^{-1} & 0 \end{pmatrix}^{-1} \begin{pmatrix} 2 & 0 \\ b^{-1} & 2^{-1} \end{pmatrix}^{-1} \begin{pmatrix} 0 & b \\ -b^{-1} & 0 \end{pmatrix} \begin{pmatrix} 2 & 0 \\ b^{-1} & 2^{-1} \end{pmatrix}$$
$$= \begin{pmatrix} 0 & 2^{-1}b \\ 2^{-1}b^{-1} & -1 \end{pmatrix}.$$

因此不妨设 $\mathfrak{N}$ 包有 $\begin{pmatrix} 0 & b \\ -b^{-1} & d \end{pmatrix}$ 而 $d \neq 0$. 于是 $\mathfrak{N}$ 含有

$$\left[\begin{pmatrix} 0 & b \\ -b^{-1} & d \end{pmatrix}^{-1} \begin{pmatrix} 2 & 0 \\ 0 & 2^{-1} \end{pmatrix}^{-1} \begin{pmatrix} 0 & b \\ -b^{-1} & d \end{pmatrix} \begin{pmatrix} 2 & 0 \\ 0 & 2^{-1} \end{pmatrix}\right]^2$$
$$= \begin{pmatrix} 4 & 3bd \\ 0 & 4 \end{pmatrix}^2 = \begin{pmatrix} 1 & -bd \\ 0 & 1 \end{pmatrix},$$

此处 $bd \neq 0$. 这就证明了我们的断言.

于是本定理可从引理 3 推出.

当 $K = F_2$ 及 F_3 时, 定理 1 并不成立. 例如, 当 $K = F_2$ 时, 我们知道 $GL_2(F_2) = SL_2(F_2) \cong \mathfrak{S}_3$(三个文字的对称群). 显然, 三个文字的交错群 $\mathscr{A}_3$ 是 $\mathfrak{S}_3$ 的一个正规子群, 但是 $\mathscr{A}_3$ 既不包在 $\mathfrak{S}_3$ 的中心 (仅由单位元素组成), 又不包含 $SL_2(F_2)$. 当 $K = F_3$ 时, $SL_2(F_3)$ 由以下 24 个元素组成:

$$\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} -1 & 0 \\ 0 & -1 \end{pmatrix}; \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}, \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix};$$
$$\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} -1 & -1 \\ 0 & -1 \end{pmatrix}; \begin{pmatrix} 1 & -1 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} -1 & 1 \\ 0 & -1 \end{pmatrix};$$
$$\begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix}, \begin{pmatrix} -1 & 0 \\ -1 & -1 \end{pmatrix}; \begin{pmatrix} 1 & 0 \\ -1 & 1 \end{pmatrix}, \begin{pmatrix} -1 & 0 \\ 1 & -1 \end{pmatrix};$$
$$\begin{pmatrix} 0 & -1 \\ 1 & 1 \end{pmatrix}, \begin{pmatrix} 0 & 1 \\ -1 & -1 \end{pmatrix}; \begin{pmatrix} 1 & -1 \\ 1 & 0 \end{pmatrix}, \begin{pmatrix} -1 & 1 \\ -1 & 0 \end{pmatrix};$$
$$\begin{pmatrix} 0 & 1 \\ -1 & 1 \end{pmatrix}, \begin{pmatrix} 0 & -1 \\ 1 & -1 \end{pmatrix}; \begin{pmatrix} 1 & 1 \\ -1 & 0 \end{pmatrix}, \begin{pmatrix} -1 & -1 \\ 1 & 0 \end{pmatrix};$$

$$\begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}, \quad \begin{pmatrix} -1 & -1 \\ -1 & 1 \end{pmatrix}; \quad \begin{pmatrix} 1 & -1 \\ -1 & -1 \end{pmatrix}, \quad \begin{pmatrix} -1 & 1 \\ 1 & 1 \end{pmatrix}.$$

可以验证下面 8 个元素:

$$\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \quad \begin{pmatrix} -1 & 0 \\ 0 & -1 \end{pmatrix}; \quad \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}, \quad \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix};$$

$$\begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}, \quad \begin{pmatrix} -1 & -1 \\ -1 & 1 \end{pmatrix}; \quad \begin{pmatrix} 1 & -1 \\ -1 & -1 \end{pmatrix}, \quad \begin{pmatrix} -1 & 1 \\ 1 & 1 \end{pmatrix}.$$

组成 $SL_2(F_3)$ 的一个正规子群.

定理 1 有一系列的推论.

定理 2 设 $K \neq F_2$ 及 $F_3, GL_2(K)$ 的正规子群如不包在它的中心之中, 一定包有 $SL_2(K)$.

定理 3 设 $K \neq F_2$ 及 $F_3, SL_2(K)$ 的正规子群如不包在它的中心之中, 一定就是 $SL_2(K)$ 本身.

这个定理可以改述为

定理 4 设 $K \neq F_2$ 及 F_3, 则 $PSL_2(K)$ 是单群.

§6 $SL_2(K)$ 的自同构

我们先讨论体 K 的特征数 $p \neq 0$ 的情形. 这时 $SL_2(K)$ 的自同构的确定有赖于将其中的抛物元素刻画出来.

定义 1 设体 K 的特征数 $p \neq 0$. $GL_2(K)$ 里的一个矩阵 $A \neq I$ 称为抛物元素, 如果 $A^p = I$.

引理 1 设体 K 的特征数 $p \neq 0$, 再设 A 为 $GL_2(K)$ 里的一个抛物元素, 于是有 $P \in GL_2(K)$, 使

$$PAP^{-1} = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}.$$

【证】 由 $A^p = I$ 推出 $(A-I)^p = 0$. 因 $A \neq I$, 故由 $A-I$ 幂零推出 $A-I$ 不是中心矩阵. 设 $A - I = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$.

如果 $c = 0$, 则由

$$(A-I)^p = \begin{pmatrix} a^p & x \\ 0 & d^p \end{pmatrix} = 0$$

推出 $a=d=0$. 所以 $A-I=\begin{pmatrix}0&b\\0&0\end{pmatrix}$, $A=\begin{pmatrix}1&b\\0&1\end{pmatrix}$. 因 $A\neq I$, 故 $b\neq 0$, 于是

$$\begin{pmatrix}1&0\\0&b\end{pmatrix}\begin{pmatrix}1&b\\0&1\end{pmatrix}\begin{pmatrix}1&0\\0&b\end{pmatrix}^{-1}=\begin{pmatrix}1&1\\0&1\end{pmatrix}.$$

如果 $c\neq 0$, 则由

$$\begin{pmatrix}1&\lambda\\0&1\end{pmatrix}\begin{pmatrix}a&b\\c&d\end{pmatrix}\begin{pmatrix}1&\lambda\\0&1\end{pmatrix}^{-1}=\begin{pmatrix}a+\lambda c&*\\c&*\end{pmatrix}$$

知可选取 λ 使 $a+\lambda c=0$. 于是不妨设 $A-I=\begin{pmatrix}0&b\\c&d\end{pmatrix}$, 而 $c\neq 0$. 因 $A-I$ 幂零, 而 $c\neq 0$, 故 $b=0$. 再由

$$(A-I)^p=\begin{pmatrix}0&0\\ *&d^p\end{pmatrix}=0$$

推出 $d=0$. 因此 $A-I=\begin{pmatrix}0&0\\c&0\end{pmatrix}$, $A=\begin{pmatrix}1&0\\c&1\end{pmatrix}$. 于是

$$\begin{pmatrix}0&1\\c&0\end{pmatrix}\begin{pmatrix}1&0\\c&1\end{pmatrix}\begin{pmatrix}0&1\\c&0\end{pmatrix}^{-1}=\begin{pmatrix}1&1\\0&1\end{pmatrix}.$$

因此引理成立.

由这个引理立刻推出 $GL_2(K)$ 中抛物元素都属于 $SL_2(K)$, 而且 $SL_2(K)$ 由其中的抛物元素生成.

引理 2　设体 K 的特征数 $p\neq 0$, 则两个不相交换的抛物元素在 $GL_2(K)$ 之下可以同时化到

$$\begin{pmatrix}1&1\\0&1\end{pmatrix}\quad 和\quad \begin{pmatrix}1&0\\\gamma&1\end{pmatrix},\quad \gamma\neq 0.$$

【证】　依引理 1, 可以假设它们已经化到了

$$\begin{pmatrix}1&1\\0&1\end{pmatrix}\quad 和\quad P\begin{pmatrix}1&1\\0&1\end{pmatrix}P^{-1}.$$

令 $P=\begin{pmatrix}a&b\\c&d\end{pmatrix}$. 首先, 我们断言 $c\neq 0$, 否则

$$\begin{pmatrix}a&b\\0&d\end{pmatrix}\begin{pmatrix}1&1\\0&1\end{pmatrix}\begin{pmatrix}a&b\\0&d\end{pmatrix}^{-1}=\begin{pmatrix}1&ad^{-1}\\0&1\end{pmatrix}$$

将与 $\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$ 相交换.

如果 $a=0$, 则

$$\begin{pmatrix} 0 & b \\ c & d \end{pmatrix}\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}\begin{pmatrix} 0 & b \\ c & d \end{pmatrix}^{-1}=\begin{pmatrix} 1 & 0 \\ cb^{-1} & 1 \end{pmatrix}.$$

如果 $a\neq 0$, 则由

$$\begin{pmatrix} 1 & s \\ 0 & 1 \end{pmatrix}\begin{pmatrix} a & b \\ c & d \end{pmatrix}=\begin{pmatrix} a+sc & b+sd \\ c & d \end{pmatrix}$$

可知, 我们可选 s 使 $a+sc=0$. 因

$$\begin{pmatrix} 1 & s \\ 0 & 1 \end{pmatrix}\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}\begin{pmatrix} 1 & s \\ 0 & 1 \end{pmatrix}^{-1}=\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix},$$

所以这个情形化到了 $a=0$ 的情形.

定理 1 设 K 的特征数 $p\neq 0$, 则 $SL_2(K)$ 的任何一个自同构必为下列两种形状之一:

(1) $$A\to PA^{\sigma}P^{-1},$$

其中 $P\in GL_2(K)$, σ 为 K 之自同构; 或

(2) $$A\to P(A'^{\tau})^{-1}P^{-1},$$

其中 τ 为 K 之反自同构.

【证】 设 $\mathscr{A}$ 为 $SL_2(K)$ 的自同构. 因 $\mathscr{A}$ 将抛物元素映到抛物元素, 故依引理 2 不妨设, 在 $\mathscr{A}$ 之下,

$$\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}\to\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix},\quad \begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix}\to\begin{pmatrix} 1 & 0 \\ \gamma & 1 \end{pmatrix}.$$

与 $\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$ 相交换的抛物元素的形状是

$$\begin{pmatrix} 1 & s \\ 0 & 1 \end{pmatrix},$$

它们组成一群, 记作 Γ_1. 与 $\begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix}$ 或 $\begin{pmatrix} 1 & 0 \\ \gamma & 1 \end{pmatrix}$ 相交换的抛物元素的形状是

$$\begin{pmatrix} 1 & 0 \\ t & 1 \end{pmatrix},$$

它们组成一群, 记作 Γ_2. 于是 $\mathscr{A}$ 将 Γ_1 映到 Γ_1, 将 Γ_2 映到 Γ_2.

现在考查 $\begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}$ 这个元素在 $\mathscr{A}$ 之下的像. 因 $\begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}$ 将 Γ_1 和 Γ_2 互换, 即

$$\begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix} \Gamma_1 = \Gamma_2 \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}.$$

在 $SL_2(K)$ 中将 Γ_1 和 Γ_2 互换的元素必为形状 $\begin{pmatrix} 0 & b \\ c & 0 \end{pmatrix}$, 故

$$\mathscr{A}\begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix} = \begin{pmatrix} 0 & b \\ c & 0 \end{pmatrix}.$$

又因 $\begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}^2 = -I$, 而 $\mathscr{A}$ 将 $(-I)$ 不变, 故 $c = -b^{-1}$. 于是

$$\mathscr{A}\begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix} = \begin{pmatrix} 0 & b \\ -b^{-1} & 0 \end{pmatrix}.$$

注意

$$\begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix} = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}\begin{pmatrix} 1 & 0 \\ -1 & 1 \end{pmatrix}\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix},$$

于是在 $\mathscr{A}$ 之下, 它映到

$$\begin{pmatrix} 0 & b \\ -b^{-1} & 0 \end{pmatrix} = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}\begin{pmatrix} 1 & 0 \\ s & 1 \end{pmatrix}\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}.$$

由此推出 $s = -1, b = 1$, 于是有

$$\mathscr{A}\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}, \quad \mathscr{A}\begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix},$$

$$\mathscr{A}\begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix} = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix},$$

由 $\mathscr{A}$ 将 Γ_1 映到 Γ_1 推出

$$\mathscr{A}\begin{pmatrix}1 & x\\0 & 1\end{pmatrix}=\begin{pmatrix}1 & x^\sigma\\0 & 1\end{pmatrix},$$

而 $x\to x^\sigma$ 为由 K 到 K 之上的映射. 因为

$$\begin{pmatrix}1 & x\\0 & 1\end{pmatrix}\begin{pmatrix}1 & y\\0 & 1\end{pmatrix}=\begin{pmatrix}1 & x+y\\0 & 1\end{pmatrix},$$

故

$$(x+y)^\sigma=x^\sigma+y^\sigma.$$

再由 $\mathscr{A}\begin{pmatrix}1 & 1\\0 & 1\end{pmatrix}=\begin{pmatrix}1 & 1\\0 & 1\end{pmatrix}$, 知 $1^\sigma=1$.

现在考查 $SL_2(K)$ 中将 Γ_1 和 Γ_2 不变的那些因素, 它们的形状为

$$\begin{pmatrix}a & 0\\0 & d\end{pmatrix},$$

而 $ad\in C$. 于是元素

$$\begin{pmatrix}x & 0\\0 & x^{-1}\end{pmatrix}=\begin{pmatrix}1 & -x\\0 & 1\end{pmatrix}\begin{pmatrix}1 & 0\\x^{-1} & 1\end{pmatrix}\begin{pmatrix}0 & 1\\-1 & 0\end{pmatrix}\begin{pmatrix}1 & 0\\x & 1\end{pmatrix}$$

在 $\mathscr{A}$ 之下就映到

$$\mathscr{A}\begin{pmatrix}x & 0\\0 & x^{-1}\end{pmatrix}=\begin{pmatrix}1 & -x^\sigma\\0 & 1\end{pmatrix}\begin{pmatrix}1 & 0\\(x^{-1})^\sigma & 1\end{pmatrix}\begin{pmatrix}0 & 1\\-1 & 0\end{pmatrix}\begin{pmatrix}1 & 0\\x^\sigma & 1\end{pmatrix}.$$

因 $\mathscr{A}\begin{pmatrix}x & 0\\0 & x^{-1}\end{pmatrix}$ 的形状为 $\begin{pmatrix}a & 0\\0 & d\end{pmatrix}$, 故由上式推出

$$1-x^\sigma(x^{-1})^\sigma=0,$$

于是 $(x^{-1})^\sigma=(x^\sigma)^{-1}$. 因之

$$\mathscr{A}\begin{pmatrix}x & 0\\0 & x^{-1}\end{pmatrix}=\begin{pmatrix}x^\sigma & 0\\0 & (x^{-1})^\sigma\end{pmatrix}.$$

再由

$$\begin{pmatrix}xyx & 0\\0 & (xyx)^{-1}\end{pmatrix}=\begin{pmatrix}x & 0\\0 & x^{-1}\end{pmatrix}\begin{pmatrix}y & 0\\0 & y^{-1}\end{pmatrix}\begin{pmatrix}x & 0\\0 & x^{-1}\end{pmatrix}$$

推出

$$(xyx)^\sigma = x^\sigma y^\sigma x^\sigma.$$

因之, σ 为 K 之半自同构. 于是 σ 为 K 之自同构或反自同构.

因 $SL_2(K)$ 由 Γ_1 及 $\begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}$ 所生成, 故如 σ 为 K 之自同构, 则

$$\mathscr{A}(A) = A^\sigma,$$

这时定理成立.

如果 σ 为 K 之反自同构, 则

$$\mathscr{A}\begin{pmatrix} 1 & x \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} 1 & x^\sigma \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}\begin{pmatrix} 1 & 0 \\ x^\sigma & 1 \end{pmatrix}^{-1}\begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}^{-1}.$$

$$\mathscr{A}\begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix} = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix} = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}\begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}^{-1}\begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}^{-1},$$

于是

$$\mathscr{A}(A) = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}(A'^\sigma)^{-1}\begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}^{-1},$$

这时定理也成立.

以下讨论 K 的特征数 $=0$ 的情况. 这时, 如 K 是域, 则 $SL_2(K)$ 的自同构仍是定理 1 中给出的. 如 K 不是域, 这时问题尚未解决.

定义 2　设 K 为特征数 $=0$ 的域. $SL_2(K)$ 中一个矩阵 A 称为抛物元素, 如果 $SL_2(K)$ 中有无限多个矩阵在 $SL_2(K)$ 之下与 A 相似而且与 A 交换.

引理 3　设 K 为特征数 $=0$ 的域. $SL_2(K)$ 中一个 $\neq \pm I$ 的元素为抛物元素的充要条件是它的特征方程有重根 $+1$ 或 -1. 因而每个抛物元素在 $SL_2(K)$ 之下相似于

$$\pm\begin{pmatrix} 1 & s \\ 0 & 1 \end{pmatrix} \quad (s \neq 0).$$

【证】　如果 $A \neq \pm I$ 而且有重根 ± 1, 则有 $P \in GL_2(K)$, 使

$$PAP^{-1} = \pm\begin{pmatrix} 1 & s \\ 0 & 1 \end{pmatrix} \quad (s \neq 0).$$

显然, 所有形如

$$\pm\begin{pmatrix} 1 & sa^2 \\ 0 & 1 \end{pmatrix} = \pm\begin{pmatrix} a & 0 \\ 0 & a^{-1} \end{pmatrix}\begin{pmatrix} 1 & s \\ 0 & 1 \end{pmatrix}\begin{pmatrix} a & 0 \\ 0 & a^{-1} \end{pmatrix}^{-1}$$

的矩阵都与 $\pm\begin{pmatrix} 1 & s \\ 0 & 1 \end{pmatrix}$ 在 $SL_2(K)$ 之下相似, 而且交换. 因之有无限多个矩阵与 A 在 $SL_2(K)$ 之下相似, 而且交换.

可是, 如果 A 有一个特征根 $\alpha \neq \pm 1$, 则我们可以在 K 的一个扩域中求得一个矩阵 P, 使

$$P^{-1}AP = \begin{pmatrix} \alpha & 0 \\ 0 & \alpha^{-1} \end{pmatrix}.$$

设 B 与 A 相似而且与 A 交换, 则由 $AB = BA$ 推出

$$P^{-1}BP = \begin{pmatrix} \beta & 0 \\ 0 & \beta^{-1} \end{pmatrix}.$$

再由 B 与 A 相似推出 $\alpha = \beta$ 或 $\alpha = \beta^{-1}$. 这样, 我们只有两个元素与 A 相似而且交换, 故 A 不是抛物元素.

引理 4 设 K 为特征数 $=0$ 的域, 则 $SL_2(K)$ 中任意两个不相交换的抛物元素在 $SL_2(K)$ 之下可以同时化到

$$\pm\begin{pmatrix} 1 & s \\ 0 & 1 \end{pmatrix}, \quad \pm\begin{pmatrix} 1 & 0 \\ t & 1 \end{pmatrix}.$$

【证】 依引理 3, 可设这两个抛物元素的形状为

$$\pm\begin{pmatrix} 1 & s \\ 0 & 1 \end{pmatrix}, \quad \begin{pmatrix} a & b \\ c & d \end{pmatrix} \quad (a+d=\pm 2, ad-bc=1).$$

因它们不交换, 故 $c \neq 0$. 因为 $(d-a)^2+4cb=0$, 我们可以求得唯一的一个元素 λ, 使

$$-c\lambda^2+(d-a)\lambda+b=0.$$

于是

$$\begin{pmatrix} 1 & \lambda \\ 0 & 1 \end{pmatrix}\begin{pmatrix} a & b \\ c & d \end{pmatrix}\begin{pmatrix} 1 & \lambda \\ 0 & 1 \end{pmatrix}^{-1}$$

就是我们所需要的形状的矩阵.

定理 2 设 K 为域, 则 $SL_2(K)$ 的自同构必为下列形状:

$$A \to PA^{\sigma}P^{-1},$$

其中 $P \in GL_2(K)$ 而 σ 为 K 之自同构.

【证】 如 K 的特征数为 $p \neq 0$, 本定理立刻由定理 1 推出. 现在设 K 的特征数为 0. 设 $\mathscr{A}$ 为 $SL_2(K)$ 的一个自同构, 任意选取 $s_0, t_0 \in K^*$, 则依引理 4, 不妨设在 $\mathscr{A}$ 之下:

$$\pm\begin{pmatrix} 1 & s_0 \\ 0 & 1 \end{pmatrix} \to \pm\begin{pmatrix} 1 & s_0^* \\ 0 & 1 \end{pmatrix}, \quad \pm\begin{pmatrix} 1 & 0 \\ t_0 & 1 \end{pmatrix} \to \pm\begin{pmatrix} 1 & 0 \\ t_0^* & 1 \end{pmatrix},$$

而 $s_0^*, t_0^* \in K^*$. $\pm\begin{pmatrix} 1 & s_0 \\ 0 & 1 \end{pmatrix}$ 在 $SL_2(K)$ 里的正常化子是为形如 $\pm\begin{pmatrix} 1 & s \\ 0 & 1 \end{pmatrix}$ 的元素组成的群, 将此群中元素皆平方之即得

$$\begin{pmatrix} 1 & 2s \\ 0 & 1 \end{pmatrix}.$$

因此 $SL_2(K)$ 的自同构就将形如

$$\begin{pmatrix} 1 & s \\ 0 & 1 \end{pmatrix}$$

的元素组成之群 Γ_1 变成它自己. 同样, 它亦将形如

$$\begin{pmatrix} 1 & 0 \\ t & 1 \end{pmatrix}$$

的元素组成的群 Γ_2 变到它自己.

设在 $\mathscr{A}$ 之下,

$$\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} \to \begin{pmatrix} 1 & \lambda_0 \\ 0 & 1 \end{pmatrix},$$

由于

$$\begin{pmatrix} 1 & 0 \\ 0 & \lambda_0 \end{pmatrix}\begin{pmatrix} 1 & \lambda_0 \\ 0 & 1 \end{pmatrix}\begin{pmatrix} 1 & 0 \\ 0 & \lambda_0 \end{pmatrix}^{-1} = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix},$$

而 $\begin{pmatrix} 1 & 0 \\ 0 & \lambda_0 \end{pmatrix}$ 将 Γ_1 和 Γ_2 不变, 故不妨设在 $\mathscr{A}$ 之下,

$$\mathscr{A}\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix},$$

$$\mathscr{A}(\Gamma_1) = \Gamma_1, \quad \mathscr{A}(\Gamma_2) = \Gamma_2.$$

然后可像定理 1 的证明那样进行下去, 即可证得本定理.

§7 $GL_2(K)$ 的自同构

引理 1 设 K 为体, 如果 $GL_2(K)$ 的一个自同构诱导出 $SL_2(K)$ 的单位自同构, 则 $GL_2(K)$ 的这个自同构必为形状

$$A \to \chi(A)A,$$

而 χ 为从 $GL_2(K)$ 到 K^* 的中心 Z^* 之中的一个同态映射, 并满足条件: 从 $\chi(\zeta I) = \zeta^{-1}$ 及 $\zeta \in Z^*$ 可导出 $\zeta = 1$.

【证】 因 $GL_2(K)$ 可以从 $SL_2(K)$ 添加形如

$$(1) \qquad \begin{pmatrix} 1 & 0 \\ 0 & \lambda \end{pmatrix} \quad (\lambda \in K^*)$$

的元素而得到, 所以只要考虑在 $GL_2(K)$ 的这个自同构之下, (1) 的像是什么. 设 $B \in SL_2(K)$, 则

$$(2) \qquad \begin{pmatrix} 1 & 0 \\ 0 & \lambda \end{pmatrix} B \begin{pmatrix} 1 & 0 \\ 0 & \lambda \end{pmatrix}^{-1} \in SL_2(K).$$

设 $\begin{pmatrix} 1 & 0 \\ 0 & \lambda \end{pmatrix}$ 在这个自同构之下的像是 C, 则因这个自同构诱导出 $SL_2(K)$ 的单位自同构, 故

$$\begin{pmatrix} 1 & 0 \\ 0 & \lambda \end{pmatrix} B \begin{pmatrix} 1 & 0 \\ 0 & \lambda \end{pmatrix}^{-1} = CBC^{-1},$$

对一切 $B \in SL_2(K)$. 于是

$$B \begin{pmatrix} 1 & 0 \\ 0 & \lambda \end{pmatrix}^{-1} C = \begin{pmatrix} 1 & 0 \\ 0 & \lambda \end{pmatrix}^{-1} CB,$$

对一切 $B \in SL_2(K)$. 由此推出

$$\begin{pmatrix} 1 & 0 \\ 0 & \lambda \end{pmatrix}^{-1} C = \rho I^{(2)} \quad (\rho \in Z^*).$$

于是

$$C = \rho \begin{pmatrix} 1 & 0 \\ 0 & \lambda \end{pmatrix},$$

由此即可推出本引理.

定理 1 设 K 为体, 则 $GL_2(K)$ 的自同构必为下列二种形状之一:

$$A \to \chi(A)PA^{\sigma}P^{-1}, \tag{3}$$

其中 $P \in GL_2(K)$, σ 为 K 之自同构, χ 适合引理 1 中条件; 或

$$A \to \chi(A)P(A'^{T})^{-1}P^{-1}, \tag{4}$$

其中 $P \in GL_2(K)$, τ 为 K 之反自同构, χ 适合引理 1 中条件.

【证】 因 $SL_2(K)$ 为 $GL_2(K)$ 的换位子群 (除开 $n=2, K=F_2$ 这一情形), 故 $GL_2(K)$ 的自同构一定诱导出 $SL_2(K)$ 的自同构 (当 $n=2, K=F_2$ 时, $GL_2(K)=SL_2(K)$). 于是, 如 K 的特征数 $p \neq 0$ 或 K 是特征数 =0 的域, 依定理 6.1 和定理 6.2, 我们有在 $GL_2(K)$ 的自同构 $\mathscr{A}$ 之下,

$$\mathscr{A}(A) = PA^{\sigma}P^{-1} \quad (A \in SL_2(K)), \tag{5}$$

其中 $P \in GL_2(K)$, σ 为 K 之自同构; 或

$$\mathscr{A}(A) = P(A'^{\tau})^{-1}P^{-1} \quad (A \in SL_2(K)), \tag{6}$$

其中 $P \in GL_2(K)$, τ 为 K 之反自同构. 如 (5) 发生, 则使 $\mathscr{A}$ 承受自同构

$$A \to (P^{-1}AP)^{\sigma^{-1}} \quad (A \in GL_2(K))$$

之后, 可设

$$\mathscr{A}(A) = A.$$

如 (6) 发生, 则使 $\mathscr{A}$ 承受反自同构

$$A \to [(P^{-1}AP)^{-1}]'^{\tau^{-1}} \quad (A \in GL_2(K))$$

之后, 可设

$$\mathscr{A}(A) = A.$$

于是本定理由引理 1 推出.

现在设 K 的特征数为零而 K 不是域. 我们知道, 如果 A 和 B 是反交换的对合, 即

$$A^2 = I, \quad B^2 = I, \quad AB = -BA,$$

则依定理 3.2, 可将 A 和 B 同时在相似变换之下化为

$$\begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix} \text{ 和 } \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}. \tag{7}$$

因此, 如果 $\mathscr{A}$ 是 $GL_2(K)$ 的一个自同构, 我们可以假定 $\mathscr{A}$ 不变 (7) 中两个矩阵.

不难证明与 (7) 中两个矩阵都相交换的 $GL_2(K)$ 中元素必具形状

$$\begin{pmatrix} \lambda & 0 \\ 0 & \lambda \end{pmatrix} \quad (\lambda \in K^*),$$

它们组成一群, 记作 Σ. 于是 $\mathscr{A}(\Sigma) = \Sigma$.

以 Z 表 K 之中心. 与 Σ 中每个元素都交换的 $GL_2(K)$ 中的矩阵必属于 $GL_2(Z)$, 而且反之, $GL_2(Z)$ 中每个元素与 Σ 中每个元素都交换. 因此 $\mathscr{A}$ 诱导出 $GL_2(Z)$ 的一个自同构, 因 $SL_2(Z)$ 是 $GL_2(Z)$ 的换位子群, 故 $\mathscr{A}$ 诱导出 $SL_2(Z)$ 的一个自同构. 依定理 6.2, 可设

$$\mathscr{A}(A) = PA^\sigma P^{-1} \quad (A \in SL_2(Z)),$$

其中 $P \in GL_2(Z)$, σ 为 Z 之自同构. 于是使 $\mathscr{A}$ 承受形如

$$A \to P^{-1}AP \quad (A \in GL_2(K))$$

的自同构之后, 可设

$$\mathscr{A}(A) = A^\sigma \quad (A \in SL_2(Z)).$$

注意 σ 为 Z 之自同构. 特别, 我们有

$$\mathscr{A}\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}, \quad \mathscr{A}\begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix},$$

$$\mathscr{A}\begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix} = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}.$$

$GL_2(K)$ 中与 $\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$ 交换而且相似的元素必为形状

$$\begin{pmatrix} 1 & x \\ 0 & 1 \end{pmatrix} \quad (x \in K^*),$$

它们组成一群, 记作 Γ_1. 我们有 $\mathscr{A}(\Gamma_1) = \Gamma_1$. 以 Γ_2 表形如

$$\begin{pmatrix} 1 & 0 \\ y & 1 \end{pmatrix} \quad (y \in K^*)$$

的元素组成的群, 同样有 $\mathscr{A}(\Gamma_2) = \Gamma_2$. 如定理 6.1 那样进行下去, 我们有

$$\mathscr{A}(A) = A^\sigma \quad (A \in SL_2(K)),$$

其中 σ 为 K 之自同构, 或我们有

$$\mathscr{A}(A)=\begin{pmatrix}0&1\\-1&0\end{pmatrix}(A'^{\tau})^{-1}\begin{pmatrix}0&1\\-1&0\end{pmatrix}^{-1}\quad(A\in SL_2(K)),$$

其中 τ 为 K 之反自同构. 于是本定理也可由引理 1 推出. 至此定理完全证毕.

§8　$SL_2^{\pm}(K)$ 的自同构

与引理 7.1 平行, 我们可以证明

引理 1　设 K 为体. 如果 $SL_2^{\pm}(K)$ 的一个自同构诱导出 $SL_2(K)$ 的单位自同构, 则 $SL_2^{\pm}(K)$ 的这个自同构必为形状

$$A\to\chi(A)A,$$

其中 χ 适合引理 7.1 中的条件.

更进一步, 如 $-1\in C$, 我们恒有 $\chi(A)=1$, 对一切 $A\in SL_2^{\pm}(K)$. 如 $-1\notin C$, 则 $\chi(A)=1$, 如 $A\in SL_2(K)$; $\chi(A)=-1$, 如 $A\notin SL_2(K)$.

定理 1　设 K 为体, 则 $SL_2^{\pm}(K)$ 的自同构必为下列两种形状之一:

(1)
$$A\to\chi(A)PA^{\sigma}P^{-1},$$

其中 σ 为 K 之自同构, $P\in GL_2(K)$ 而 χ 适合引理 7.1 的条件; 或

(2)
$$A\to\chi(A)P(A'^{\tau})^{-1}P^{-1},$$

其中 τ 为 K 之反自同构, $P\in GL_2(K)$, 而 χ 适合引理 7.1 的条件.

【证】　如 K 的特征数 $p\neq 0$ 或 K 是域, 本定理可仿照定理 7.1 推出. 现在设 K 是特征数 $=0$ 的体而不是域. 设 $\mathscr{A}$ 为 $SL_2^{\pm}(K)$ 的一个自同构. 像定理 7.1 的证明一样, 不妨设

$$\mathscr{A}\begin{pmatrix}1&0\\0&-1\end{pmatrix}=\begin{pmatrix}1&0\\0&-1\end{pmatrix},\quad \mathscr{A}\begin{pmatrix}0&1\\1&0\end{pmatrix}=\begin{pmatrix}0&1\\1&0\end{pmatrix}.$$

$SL_2^{\pm}(K)$ 中与 $\begin{pmatrix}1&0\\0&-1\end{pmatrix}$ 和 $\begin{pmatrix}0&1\\1&0\end{pmatrix}$ 都交换的元素必为形状

$$\begin{pmatrix}\lambda&0\\0&\lambda\end{pmatrix},$$

而 λ^2 或 $-\lambda^2 \in C$, 它们组成一群, 记作 Σ. Σ 在 $SL_2^{\pm}(K)$ 中的中心化子 Γ 中的元素必为形状

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix},$$

而 $a\lambda = \lambda a, b\lambda = \lambda b, c\lambda = \lambda c, d\lambda = \lambda d$ 对一切 λ 适合条件 $\lambda^2 \in C$ 或 $-\lambda^2 \in C$. 因之, $a\lambda = \lambda a$ 对一切 $\lambda \in C$, 故 $a \in Z$. 同理 $b, c, d \in Z$. 显然

$$GL_2(Z) \supset \Gamma \supset SL_2(Z).$$

由于 Γ 的换位子群为 $SL_2(Z)$, 故 $\mathscr{A}$ 诱导出 $SL_2(Z)$ 的一个自同构, 于是像定理 7.1 那样进行下去, 本定理即得证.

【备注】 我们知道, 如 $-1 \in C$, 则 $SL_2(K) = SL_2^{\pm}(K)$. 因此只有当 K 是特征数 $=0$ 的不可交换的体而 $-1 \notin C$ 时, $SL_2(K)$ 的自同构的形状没有被决定出来.

§9 $PSL_2(K), PGL_2(K)$ 及 $PSL_2^{\pm}(K)$ 的自同构

我们先讨论 $PSL_2(K)$ 的自同构. 我们从 K 的特征数 $p \neq 0$ 的情形开始.

定义 1 设 K 是特征数 $p \neq 0$ 的体. $PSL_2(K)$ 中的一个矩阵 $A \neq I$ 称为抛物元素, 如果 $A^p = \gamma I$, 而 γ 为 K 的一个中心元素, γ 称为 A 的标量. (当然 $\gamma^2 \in Z$.)

显然, $PSL_2(K)$ 的自同构必将抛物元素变到抛物元素.

设 A 和 B 为两抛物元素, 即 $A^p = \alpha I, B^p = \beta I$, 而 α 和 β 都是中心元素. 如果 A 和 B 在 $PSL_2(K)$ 中共轭, 即 $PSL_2(K)$ 中有一矩阵 P, 使

$$PAP^{-1} = \gamma B,$$

而 γ 为 K 的中心元素, 则

$$\alpha I = A^p = PA^pP^{-1} = \gamma^p B^p = \gamma^p \beta I,$$

因之 $\alpha = \gamma^p \beta$. 这说明两个共轭抛物元素的标量仅差一个中心元素的 p 次幂. 因为 B 和 γB 表示同一射影变换, 因此不妨假定共轭抛物元素具有相同的标量.

设 A 是 $PSL_2(K)$ 中的一个抛物元素, $A^p = \alpha I$. 设 B 为 $PSL_2(K)$ 中与 A 相交换的元素, 即 $AB = \delta BA$, 而 δ 为 K 的中心元素. 因为

$$\alpha B = A^p B = \delta^p BA^p = \delta^p \alpha B,$$

所以 $\delta^p = 1$, 因而 $\delta = 1$, 于是 $AB = BA$.

现在我们把 $PSL_2(K)$ 中的抛物元素分成共轭元素类的集 Γ_α, 而 Γ_α 表以 α 为标量的那些抛物元素, α 跑过 K 的中心的乘法群对其 p 次幂元素所组成的子群

的陪集的完全代表系的一个子集. 显然, Γ_α 可以由几个共轭元素类组成, 可是一个共轭元素类只可能属于唯一的一个 Γ_α.

Γ_1 是最主要的一个集合, 它包含两个 Abel 子群 Σ_1 和 Σ_2, Σ_1 由一切形如

$$\begin{pmatrix} 1 & \lambda \\ 0 & 1 \end{pmatrix} \quad (\lambda \in K)$$

的元素组成, 而 Σ_2 由一切形如

$$\begin{pmatrix} 1 & \lambda \\ \mu & 1 \end{pmatrix} \quad (\mu \in K)$$

的元素组成. 我们断言, 使 $PSL_2(K)$ 的自同构承受一个由 $GL_2(K)$ 中元素所引起的自同构

$$\bar{X} \to \bar{P}\bar{X}\bar{P}^{-1} \quad (P \in GL_2(K))$$

之后, 可以假定

$$\Sigma_1 \to \Sigma_1 \quad 及 \quad \Sigma_2 \to \Sigma_2.$$

为了证明这个断言, 我们分以下几个情形来考查.

I. K 的元素个数大于 5, 而其特征数 $\neq 2$. 这时 Γ_1 被 $PSL_2(K)$ 的每个自同构都不变. 实际上, 以 A 表 Γ_1 中任一元素, 依引理 6.1, 有一个矩阵 $P \in GL_2(K)$, 使

$$PAP^{-1} = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}.$$

因 K 中元素个数大于 5, 所以可以在 K 中找到一个元素 $t \neq 0$, 使得 $t^4 - 1 \neq 0$. 令

$$\lambda = \frac{2t}{1+t^2}, \quad \mu = \frac{t^2-1}{1+t^2},$$

则

$$\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} \quad 和 \quad \begin{pmatrix} 1 & \lambda^2 \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} \lambda & 0 \\ 0 & \lambda^{-1} \end{pmatrix}\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}\begin{pmatrix} \lambda & 0 \\ 0 & \lambda^{-1} \end{pmatrix}^{-1}$$

就是 Γ_1 中两个互相共轭而且交换的抛物元素, 而

$$\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}\begin{pmatrix} 1 & \lambda^2 \\ 0 & 1 \end{pmatrix}^{-1} = \begin{pmatrix} 1 & 1-\lambda^2 \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} 1 & \mu^2 \\ 0 & 1 \end{pmatrix}$$

亦与上面两个元素共轭, 置

$$B = P^{-1}\begin{pmatrix} 1 & \lambda^2 \\ 0 & 1 \end{pmatrix}P, \quad C = P^{-1}\begin{pmatrix} 1 & \mu^2 \\ 0 & 1 \end{pmatrix}P,$$

则 A, B, C 是 Γ_1 中的三个互相共轭而且互相交换的元素, 并且

$$AB^{-1} = C.$$

在 $PSL_2(K)$ 的一个自同构之下, 设

$$A \to A_1, \quad B \to B_1, \quad C \to C_1,$$

则 A_1, B_1, C_1 是三个互相共轭而且互相交换的元素, 并且

$$A_1 B_1^{-1} = C_1.$$

假定 $A_1, B_1, C_1 \in \Gamma_\alpha$, 则

$$C_1^p = (A_1 B_1^{-1})^p = \alpha I \alpha^{-1} I = I,$$

因之, $\alpha = 1$, 即 $A_1 \in \Gamma_1$. 因之 Γ_1 在 $PSL_2(K)$ 的自同构的作用下不变.

今考虑

$$\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} \quad \text{和} \quad \begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix},$$

它们是 Γ_1 中不相交换的两个抛物元素. 依引理 6.2, 行施由 $GL_2(K)$ 中一个元素诱导出的一个自同构之后, 可以设在 $PSL_2(K)$ 的自同构之下,

$$\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} \to \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} \quad \text{及} \quad \begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix} \to \begin{pmatrix} 1 & 0 \\ s & 1 \end{pmatrix}.$$

由于 Σ_1 是 Γ_1 中与 $\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$ 相交换的元素的全体, 而 Σ_2 是 Γ_1 中与 $\begin{pmatrix} 1 & 0 \\ s & 1 \end{pmatrix}$ 相交换的元素的全体, 所以在 $PSL_2(K)$ 的这个自同构之下,

$$\Sigma_1 \to \Sigma_1, \quad \Sigma_2 \to \Sigma_2.$$

II. K 的特征数 $p = 2$. 这时, Γ_1 也被 $PSL_2(K)$ 的自同构所不变. 因为, 如果 K 只有两个元素, 我们只有一个 Γ_α, 就是 Γ_1. 如果 K 多于两个元素, 则 K 中有一元素 $t \neq 0, 1$, 以 A 表 Γ_1 中任一元素, 则依引理 6.1, 可以把 A 写作

$$A = P \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} P^{-1} \quad (P \in GL_2(K)).$$

于是

$$A = P \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} P^{-1}, \quad B = P \begin{pmatrix} 1 & t^2 \\ 0 & 1 \end{pmatrix} P^{-1},$$

$$C = P\begin{pmatrix} 1 & (1+t)^2 \\ 0 & 1 \end{pmatrix} P^{-1}$$

是 $PSL_2(K)$ 中三个互相共轭而且互相交换的元素, 并且

$$AB^{-1} = C,$$

因之, 利用情形 I 同样的论证, 可知 Γ_1 被 $PSL_2(K)$ 的每一个自同构的作用下不变. 再像情形 I 一样进行下去, 我们可假定在 $PSL_2(K)$ 的自同构之下, 有

$$\Sigma_1 \to \Sigma_1 \quad 及 \quad \Sigma_2 \to \Sigma_2.$$

III. K 只有 3 个元素或 5 个元素. 我们有两个 Γ_α, 即 Γ_1 和 Γ_{-1}. 因为由 $A^p = \alpha I$ 和 $A \in SL_2(K)$, 推知 $\alpha^2 = 1$, 故 $\alpha = 1$ 或 $\alpha = -1$.

今 $PSL_2(K)$ 中含于 Γ_1 或 Γ_{-1} 的抛物元素 A 恒适合

$$A^{2p} = I.$$

不难证明, A 为抛物元素当且仅当 A 在 $SL_2(K)$ 之下相似于形如

$$\pm\begin{pmatrix} 1 & s \\ 0 & 1 \end{pmatrix}$$

的一个元素. 因此, 像引理 6.2 一样可以证明, 任意两个不交换的抛物元素在 $SL_2(K)$ 的自同构之下可以同时化到

$$\pm\begin{pmatrix} 1 & s \\ 0 & 1 \end{pmatrix} \quad 和 \quad \pm\begin{pmatrix} 1 & 0 \\ t & 1 \end{pmatrix}.$$

因此, 我们的断言可以像定理 6.1 的证明中那样来证明.

因此, 我们有, 除开可能行施一个由 $GL_2(K)$ 的元素所诱导出的自同构之外, 在 $PSL_2(K)$ 的自同构之下, 恒有

$$\Sigma_1 \to \Sigma_1 \quad 及 \quad \Sigma_2 \to \Sigma_2.$$

更进一步, 我们可以假定

$$\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} \to \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix},$$

实际上, 如果

$$\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} \to \begin{pmatrix} 1 & s \\ 0 & 1 \end{pmatrix},$$

则映射

$$X \to \begin{pmatrix} 1 & 0 \\ 0 & s \end{pmatrix} X \begin{pmatrix} 1 & 0 \\ 0 & s \end{pmatrix}^{-1}$$

将不变 Σ_1 和 Σ_2 而将 $\begin{pmatrix} 1 & s \\ 0 & 1 \end{pmatrix}$ 变到 $\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$.

考查元素 $\begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}$. 因为它互换 Σ_1 和 Σ_2, 所以它映到形如

$$\begin{pmatrix} 0 & b \\ -c & 0 \end{pmatrix} \quad (bc \in C)$$

的一个元素. 因为

$$\left[\begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}\right]^3 = I,$$

所以

$$\left[\begin{pmatrix} 0 & b \\ -c & 0 \end{pmatrix}\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}\right]^3 = \begin{pmatrix} bc^2 & -bcb+bc^2 \\ cbc-c^3 & cbc+c^2b-c^3 \end{pmatrix} = \gamma I.$$

由此推出 $b=c$ 而且 $b^3 \in Z$. 再者, 因为

$$\begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}^2 = -I.$$

所以

$$\begin{pmatrix} 0 & b \\ -b & 0 \end{pmatrix}^2 = \begin{pmatrix} -b^2 & 0 \\ 0 & -b^2 \end{pmatrix} = \delta I,$$

因之, $b^2 \in Z$. 于是 $b \in Z$, 因而在已知的自同构之下,

$$\begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix} \to \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}.$$

像定理 6.1 的证明那样进行下去就可以证明

定理 1 设 K 为特征数 $p \neq 0$ 的体, 则 $PSL_2(K)$ 的每个自同构都由 $SL_2(K)$ 的一个自同构诱导出来.

我们也有

定理 2 设 K 为域, 则 $PSL_2(K)$ 的每个自同构都由 $SL_2(K)$ 的一个自同构诱导出来.

如果 K 的特征数 $p \neq 0$, 本定理可由定理 1 推出. 如果 K 的特征数为 0, 则像定义 6.2 一样, 我们定义 $PSL_2(K)$ 中一元素 A 为抛物元素, 若有无限多个矩阵与 A 相似且与 A 交换. 然后引理 6.3 及 6.4 可同样加以证明, 再像定理 6.2 的证明一样即可证明本定理.

从定理 1 和定理 2 立即推出

定理 3　设 K 是特征数 $p \neq 0$ 的体或 K 是域, 则 $PGL_2(K)$ (以及 $PSL_2^{\pm}(K)$) 的每个自同构都由 $GL_2(K)$ (相应地由 $SL_2^{\pm}(K)$) 的一个自同构诱导出来.

【备注】　除了定理 1, 2, 3 所获结果外, 当 K 是特征数为 0 的不可交换的体时, 二级射影线性群的自同构尚未决定出来.

第三章　向量空间, 矩阵和行列式

§1　矩阵的代数

设 K 为体, 不一定是域, K 上 mn 个元素 a_{ij} $(i=1,2,\cdots,m;j=1,2,\cdots,n)$ 排成一个长方形

$$A=\begin{pmatrix} a_{11} & a_{12} & \cdots & a_{1n} \\ a_{21} & a_{22} & \cdots & a_{2n} \\ \cdots & \cdots & \cdots & \cdots \\ a_{m1} & a_{m2} & \cdots & a_{mn} \end{pmatrix}=(a_{ij})_{1\leqslant i\leqslant m,1\leqslant j\leqslant n},$$

称为 K 上的一个 m 行 n 列的矩阵, 或 $m\times n$ 矩阵. 数对 (m,n) 称为 A 的型. (n,n) 型的矩阵称为 $n\times n$ 方阵, 或简称为 n 行矩阵.

两个 $m\times n$ 矩阵 $A=(a_{ij})$ 及 $B=(b_{ij})$ 的和 $C=(c_{ij})$ 由下式所定义:

$$c_{ij}=a_{ij}+b_{ij}\quad (i=1,2,\cdots,m;j=1,2,\cdots,n).$$

C 亦为 $m\times n$ 矩阵. 应注意者为我们只定义了同型矩阵之和. 显然, 所有 $m\times n$ 矩阵的全体对加法而言组成一群, 此群的零元素即为所有系数都等于零的 $m\times n$ 矩阵, 我们把这个矩阵记作 $0^{(m,n)}$, 或简记作 0.

一个 $m\times n$ 矩阵 $A=(a_{ij})$ 和一个 $n\times l$ 矩阵 $B=(b_{ij})$ 的乘积 $C=(c_{ij})$ 由下式所定义:

$$c_{ij}=\sum_{k=1}^{n}a_{ik}b_{kj}\quad (i=1,2,\cdots,m;j=1,2,\cdots,l).$$

应注意者, 一个 $m\times n$ 矩阵与一个 $q\times l$ 矩阵之积仅当 $n=q$ 时才有定义, 而结果是一个 $m\times l$ 矩阵. 如果 A 和 B 都是方阵, 则 AB 和 BA 都有定义. 可是即使 K 是域的话, 它们也不见得相等.

K 上所有矩阵并不组成一环, 因为加法和乘法并不是对于任意两个矩阵都有定义的. 可是, 我们可以证明:

(1)　　$$(AB)C=A(BC)\quad (结合律),$$

(2)　　$$A(B+C)=AB+AC\quad (分配律),$$

(3) $$(B+C)A = BA + CA \quad (\text{分配律}),$$

只要 (1), (2) 和 (3) 里的运算是定义了的话.

然而, K 上 n 行矩阵的全体组成一环, 称为 K 上 n 级全矩阵环. 这个环绝不交换而且有零因子, 可是这个环有单位元素, 即单位矩阵

$$I^{(n)} = \begin{pmatrix} 1 & 0 & \cdots & 0 \\ 0 & 1 & \cdots & 0 \\ \cdots & \cdots & \cdots & \cdots \\ 0 & 0 & \cdots & 1 \end{pmatrix} = (\delta_{ij})_{1\leqslant i,j\leqslant n},$$

而其中

$$\delta_{ij} = \begin{cases} 0 & \text{如果} i \neq j; \\ 1 & \text{如果} i = j. \end{cases}$$

这样定义的符号 δ_{ij} 在数学中常遇到, 称为 Kronecker delta.

一个 $n\times n$ 矩阵 A 称为可逆矩阵, 如果它有一个逆元素 A^{-1} 适合:

$$AA^{-1} = A^{-1}A = I^{(n)}.$$

不难证明, 逆元素是唯一的.

如果 A 和 B 都是可逆矩阵, 则 AB 也是可逆矩阵, 而其逆为 $B^{-1}A^{-1}$. 因为, 依结合律有

$$(AB)(B^{-1}A^{-1}) = A(BB^{-1})A^{-1} = AI^{(n)}A^{-1} = I^{(n)}$$

以及

$$(B^{-1}A^{-1})(AB) = B^{-1}(A^{-1}A)B = B^{-1}I^{(n)}B = I^{(n)}.$$

因此我们可以写

$$(AB)^{-1} = B^{-1}A^{-1}.$$

所以 n 行可逆矩阵对乘法而言组成一群, 这个群称为体 K 上的 n 级一般线性群, 记作 $GL_n(K)$.

设 A 为 $m\times n$ 矩阵, 而 $i_1, i_2, \cdots, i_{m'}; j_1, j_2, \cdots, j_{n'}$ 为适合条件

$$1 \leqslant i_1 < i_2 < \cdots < i_{m'} \leqslant m,$$
$$1 \leqslant j_1 < j_2 < \cdots < j_{n'} \leqslant n$$

的两组整数, 则我们可以从 A 得到一个 (m', n') 型的新矩阵, 这个新矩阵是从 A 删去 A 中不在第 $i_1, i_2, \cdots, i_{m'}$ 行及第 $j_1, j_2, \cdots, j_{n'}$ 列的元素而得到的. 这样得到的矩阵称为 A 的一个子矩阵.

今以 $m_1, m_2, \cdots, m_s; n_1, n_2, \cdots, n_t$ 表 $s+t$ 个正整数, 且适合条件

$$\sum_{i=1}^{s} m_i = m, \quad \sum_{i=1}^{t} n_i = n;$$

以 A_{ij} 表 A 的那个子矩阵, 其元素位于 A 中

$$第 \left(\sum_{k=1}^{i-1} m_k + 1\right), \left(\sum_{k=1}^{i-1} m_k + 2\right), \cdots, \left(\sum_{k=1}^{i} m_k\right) 行$$

及

$$第 \left(\sum_{k=1}^{j-1} n_k + 1\right), \left(\sum_{k=1}^{j-1} n_k + 2\right), \cdots, \left(\sum_{k=1}^{j} n_k\right) 列,$$

则子矩阵 A_{ij} 是 (m_i, n_j) 型的矩阵. 我们可以将 A 写作

$$A = \begin{pmatrix} A_{11} & A_{12} & \cdots & A_{1t} \\ A_{21} & A_{22} & \cdots & A_{2t} \\ \cdots & \cdots & \cdots & \cdots \\ A_{s1} & A_{s2} & \cdots & A_{st} \end{pmatrix}.$$

我们这时说 A 对应于正整数 $m_1, \cdots, m_s; n_1, \cdots, n_t$ 分成了矩阵块.

设 B 为 $n \times l$ 矩阵, 以 $l_1, \cdots, l_r$ 表适合条件 $\sum\limits_{i=1}^{r} l_i = l$ 的一组正整数. 我们也可以将 B 依正整数 $n_1, \cdots, n_t; l_1, \cdots, l_r$ 分成矩阵块如下:

$$B = \begin{pmatrix} B_{11} & B_{12} & \cdots & B_{1r} \\ B_{21} & B_{22} & \cdots & B_{2r} \\ \cdots & \cdots & \cdots & \cdots \\ B_{t1} & B_{t2} & \cdots & B_{tr} \end{pmatrix}.$$

今 A_{ik} 为 $m_i \times n_k$ 矩阵, 而 B_{kj} 为 $n_k \times l_j$ 矩阵, 所以 $A_{ik}B_{kj}$ 有定义, 而且是一个 $m_i \times l_j$ 矩阵. 我们可用公式

$$C_{ij} = \sum_{k=1}^{t} A_{ik} B_{kj} \tag{4}$$

来定义一个 $m_i \times l_j$ 矩阵 C_{ij}, C_{ij} 中 p 行 q 列的元素为

$$\sum_{\lambda=1}^{n} a_{h\lambda} b_{\lambda k},$$

而其中

$$h=\sum_{a=1}^{i-1}m_a+p, k=\sum_{a=1}^{j-1}l_a+q.$$

于是

$$C=\begin{pmatrix} C_{11} & C_{12} & \cdots & C_{1r} \\ C_{21} & C_{22} & \cdots & C_{2r} \\ \cdots & \cdots & \cdots & \cdots \\ C_{s1} & C_{s2} & \cdots & C_{sr} \end{pmatrix}.$$

就是矩阵 $C=AB$ 依正整数 $m_1,\cdots,m_s;l_1,\cdots,l_r$ 所分成的矩阵块. 因此我们可以把 A 和 B 分别看作是 $s\times t$ 和 $t\times r$ 的矩阵, 而其元素为矩阵, 同时它们的积由 (4) 式所定义. 但应注意, 这种方法只在 A 和 B 中子矩阵是依上面所述的方法选出来的时候才可能.

类似于上面的道理, 但却比上面的道理要简单得多, 我们可以把两个 $m\times n$ 矩阵依同样一组正整数分成矩阵块:

$$A=\begin{pmatrix} A_{11} & A_{12} & \cdots & A_{1t} \\ A_{21} & A_{22} & \cdots & A_{2t} \\ \cdots & \cdots & \cdots & \cdots \\ A_{s1} & A_{s2} & \cdots & A_{st} \end{pmatrix},$$

$$B=\begin{pmatrix} B_{11} & B_{12} & \cdots & B_{1t} \\ B_{21} & B_{22} & \cdots & B_{2t} \\ \cdots & \cdots & \cdots & \cdots \\ B_{s1} & B_{s2} & \cdots & B_{st} \end{pmatrix}.$$

而有

$$A+B=\begin{pmatrix} A_{11}+B_{11} & A_{12}+B_{12} & \cdots & A_{1t}+B_{1t} \\ A_{21}+B_{21} & A_{22}+B_{22} & \cdots & A_{2t}+B_{2t} \\ \cdots & \cdots & \cdots & \cdots \\ A_{s1}+B_{s1} & A_{s2}+B_{s2} & \cdots & A_{st}+B_{st} \end{pmatrix}.$$

今后, 将矩阵分成矩阵块的方法会常用到.

§2　向 量 空 间

在上面一节里我们讨论了体 K 上的矩阵, 我们现在特别把 K 上的 $1\times n$ 矩阵叫做 K 上的 n 维向量. 所有 n 维向量之全体称为 K 上的 n 维向量空间 (或行空

间), 而记作 V_n. 依上节之结果, 或者直接来验证, 都可以得出, V_n 为加法 Abel 群. 这个群的零元素 $(0,0,\cdots,0)$ 称为零向量. 再者, 如果我们把 K 中的一个元素 a 看作是一个 1×1 向量, 则有以下诸性质:

I. au(u 被 a 乘的乘积) 在 V_n 中, 只要 u 在 V_n 中而 a 在 K 中;

II. $a(u+v)=au+bv$;

III. $(a+b)u=au+bu$;

IV. $a(bu)=(ab)u$;

V. $1\cdot u=u$,

对于 K 中任意元素 a,b 和 V_n 中任意元素 u,v.

VI. V_n 中任一向量都是下列 n 个向量:

$$e_1=(1,0,0,\cdots,0);\quad e_2=(0,1,0,\cdots,0);\cdots;\quad e_n=(0,0,0,\cdots,1)$$

的线性组合, 即如果

$$u=(a_1,a_2,a_3,\cdots,a_n),$$

则

$$u=a_1e_1+a_2e_2+a_3e_3+\cdots+a_ne_n.$$

定义 1 V_n 中 r 个向量 $u_1,u_2,\cdots,u_r$ 称为在 K 上线性相关, 如果在 K 中有 r 个不全为零的元素 $a_1,a_2,\cdots,a_r$, 使得

$$a_1u_1+a_2u_2+\cdots+a_ru_r=0;$$

否则, 它们就称为线性无关, 也说由它们所组成的向量集合线性无关.

由此定义立即推出, V_n 中任何含 $(0,0,\cdots,0)$ 的有限向量集合都线性相关, 因为如果这个集合中除开 $(0,0,\cdots,0)$ 之外还有 $u_1,u_2,\cdots,u_r$, 则有

$$a\cdot 0+0\cdot u_1+0\cdot u_2+\cdots+0\cdot u_r=0\quad 而 a\neq 0.$$

我们也可证明: 如果 $u_1,u_2,\cdots,u_r$ 线性无关, 则它的任一子集 $u_{i_1},u_{i_2},\cdots,u_{i_s}$ 亦线性无关.

定义 2 V_n 中某一向量 v 如可表成 $v=a_1u_1+\cdots+a_ru_r$, 而其中 $a_1,\cdots,a_r\in K$; $u_1,\cdots,u_r\in V_n$, 我们就说 v 线性相关于 $u_1,\cdots,u_r$, 或 v 是 $u_1,\cdots,u_r$ 的线性组合.

V_n 中线性相关于 r 个已知向量 $u_1,\cdots,u_r$ 的所有向量的全体记作 $L(u_1,\cdots,u_r)$. 显然, $L(u_1,\cdots,u_r)$ 为加法 Abel 群; 而且如果 $u\in L(u_1,\cdots,u_r)$, 则对于任一 $a\in K$, 有 $au\in L(u_1,\cdots,u_r)$. 一般地, 我们可以给出下述

定义 3　V_n 的一个加法子群 L 称为 V_n 的一个子空间, 如果它具有性质: 由 $a \in K$ 及 $v \in L$ 可推出 $av \in L$. 如果 L 仅含零向量, 则 L 称为 V_n 的零子空间; 否则就称为 L 的一个非零子空间.

于是 $L(u_1, \cdots, u_r)$ 就是 V_n 的一个子空间.

定义 4　如果 $L = L(u_1, \cdots, u_r)$, 则 $u_1, \cdots, u_r$ 称为 L 的一组生成元, L 称为由 $u_1, \cdots, u_r$ 所生成; 如果 $u_1, \cdots, u_r$ 线性无关, 则这组生成元就称为一组基.

以下诸定理是上述定义的直接推论.

定理 1　如果 $u_1, \cdots, u_r$ 线性无关, 则 $L(u_1, \cdots, u_r)$ 中任一向量 v 的表示法 $v = a_1u_1 + \cdots + a_ru_r$ 是唯一的; 反之, 如果这种表示法对于 $L(u_2, \cdots, u_r)$ 中任一元素是唯一的, 则 $u_1, \cdots, u_r$ 线性无关.

【证】　如果 $L(u_1, \cdots, u_r)$ 中的向量 v 有两种表示法:

$$v = a_1u_1 + a_2u_2 + \cdots + a_ru_r$$

及

$$v = b_1u_1 + b_2u_2 + \cdots + b_ru_r,$$

则从第一式减去第二式得

$$0 = (a_1 - b_1)u_1 + (a_2 - b_2)u_2 + \cdots + (a_r - b_r)u_r.$$

因为 $u_1, u_2, \cdots, u_r$ 线性无关, 所以

$$a_i = b_i \quad (i = 1, 2, \cdots, r).$$

反之, 假定 $L(u_1, u_2, \cdots, u_r)$ 中任意选取的元素 v 的表示法

$$v = b_1u_1 + b_2u_2 + \cdots + b_ru_r$$

是唯一的. 如果

$$a_1u_1 + a_2u_2 + \cdots + a_ru_r = 0,$$

则将以上两式相加得

$$v = (a_1 + b_1)u_1 + (a_2 + b_2)u_2 + \cdots + (a_r + b_r)u_r.$$

于是从

$$a_i + b_i = b_i \quad (i = 1, 2, \cdots, r)$$

就可推出

$$a_i = 0 \quad (i = 1, 2, \cdots, r).$$

这就证明了 $u_1, u_2, \cdots, u_r$ 线性无关.

定理 2 如果 $v_1, \cdots, v_s$ 属于 $L(u_1, \cdots, u_r)$, 则 w 属于 $L(v_1, \cdots, v_s)$, 则 w 亦属于 $L(u_1, \cdots, u_r)$.

【证】 由

$$v_j = \sum_{k=1}^{r} a_{jk} u_k \text{和} w = \sum_{j=1}^{s} b_j v_j$$

可推出

$$w = \sum_{j=1}^{s} b_j v_j = \sum_{j=1}^{s} b_j \sum_{k=1}^{r} a_{jk} u_k = \sum_{k=1}^{r} \left(\sum_{j=1}^{s} b_j a_{jk} \right) u_k.$$

以下定理至为重要.

定理 3 (Steinitz **替换定理**) 设 $v_1, \cdots, v_s$ 为 $L(u_1, \cdots, u_r)$ 中 s 个线性无关的元素, 则 $u_1, \cdots, u_r$ 中有一个子集 $u_{i_1}, \cdots, u_{i_s}$, 使得: 如果我们用 $v_1, \cdots, v_s$ 来替换 $u_1, \cdots, u_r$ 中这个子集, 则这样得到的新集亦为 $L(u_1, \cdots, u_r)$ 的一组生成元.

【证】 我们用归纳法对 s 来证明这个定理. 当 $s = 0$ 时, 定理显然成立; 设 $s > 0$, 并假定定理对于 $s-1$ 成立, 于是我们可以假定集合 $u_1, \cdots, u_r$ 中有 $s-1$ 个向量 $u_{i_1}, \cdots, u_{i_{s-1}}$ 存在, 而它们可以用 $v_1, \cdots, v_{s-1}$ 来替换, 使得

$$L(u_1, \cdots, u_r) = L(v_1, \cdots, v_{s-1}, u_{i_s}, \cdots, u_{i_r}),$$

而 $i_1, i_2, \cdots, i_r$ 为 $1, 2, \cdots, r$ 的一个重新排列. 因为 v_s 属于 $L(u_1, \cdots, u_r)$, 所以

$$(1) \qquad v_s = a_1 v_1 + \cdots + a_{s-1} v_{s-1} + a_s u_{i_s} + \cdots + a_r u_{i_r},$$

而其中 $a_s, \cdots, a_r$ 不能全为 K 中的零元素, 因为否则 (1) 就将是线性无关的向量 $v_1, \cdots, v_s$ 间的一个线性关系. 不失去普遍性, 我们可以假定已如此选取了脚标 $i_s, \cdots, i_r$, 使得 $a_s \neq 0$, 于是

$$(2) \qquad u_{i_s} = -a_s^{-1} a_1 v_1 - \cdots - a_s^{-1} a_{s-1} v_{s-1} + a_s^{-1} v_s$$

$$-a_s^{-1} a_{s+1} u_{i_{s+1}} - \cdots - a_s^{-1} a_r u_{i_r}.$$

今 $v_1, \cdots, v_{s-1}, v_s, u_{i_{s+1}}, \cdots, \mu_{i_r}$ 属于 $L(v_1, \cdots, v_{s-1}, u_{i_s}, \cdots, u_{i_r})$, 因之, 依定理 2 就有

$$L(v_1, \cdots, v_{s-1}, v_s, u_{i_{s+1}}, \cdots, u_{i_r}) \subseteq L(v_1, \cdots, v_{s-1}, u_{i_s}, \cdots, u_{i_r}).$$

可是反之, 由 (2) 亦可推出 u_{i_s} 属于 $L(v_1,\cdots,v_{s-1},v_s,u_{i_{s+1}},\cdots,u_{i_r})$, 因之

$$L(u_1,\cdots,u_r)=L(v_1,\cdots,v_{s-1},u_{i_s},\cdots,u_{i_r})$$
$$=L(v_1,\cdots,v_{s-1},v_s,u_{i_{s+1}},\cdots,u_{i_r}).$$

于是, 本定理证毕.

我们可从定理 3 马上推出下述

定理 4　$L(u_1,\cdots,u_r)$ 的任何线性无关子集至多含有 r 个向量. 特别, $V_n=L(e_1,\cdots,e_n)$ 的任何线性无关子集至多含有 n 个向量.

定理 5　V_n 的任何非零子空间 L 都有基, 而基中所含向量个数 $r\leqslant n$; 换言之, L 中有 $r(\leqslant n)$ 个线性无关向量 $u_1,\cdots,u_r$, 使得 $L=L(u_1,\cdots,u_r)$.

【证】　在 L 中选取一个非零向量 u_1, 依子空间之定义可知, L 包有所有向量 a_1u_1, 而 a_1 取遍 K 中所有元素. 如果 $L=L(u_1)$, 则定理得证; 否则, L 将有一个向量 $u_2\notin L(u_1)$, 于是 $L(u_1,u_2)\subseteq L$, 且 u_1,u_2 线性无关. 现在假定 $L(u_1,\cdots,u_{s-1})$ 已经造好了, 而其中 $u_1,\cdots,u_{s-1}$ 为 L 中线性无关向量组. 如果 $L=L(u_1,\cdots,u_{s-1})$, 则定理得证; 否则, 以 u_s 表 L 中不属于 $L(u_1,\cdots,u_{s-1})$ 的一个向量, 于是 $u_1,\cdots,u_s$ 线性无关. 因为否则我们就有不全为零的 K 中元素 $a_1,\cdots,a_s$, 使得 $a_1u_1+\cdots+a_su_s=0$, 因为 $u_1,\cdots,u_{s-1}$ 线性无关, 所以必是 $a_s\neq 0$, 于是

$$u_s=-a_s^{-1}(a_1u_1+\cdots+a_{s-1}u_{s-1})\in L(u_1,\cdots,u_{s-1}),$$

此为一矛盾. 依定理 4, s 不能超过 n, 因之定理得证.

定理 6　如果 $u_1,\cdots,u_r$ 为 V_n 中一个非零子空间 L 的一组基, 则 L 的任意一组基中亦恰含 r 个线性无关的向量; 换言之, 一子空间的基中元素的个数对于所有基而言都是相等的. 更进一步, 如果 $v_1,\cdots,v_r$ 为 L 中任意 r 个线性无关的元素, 则

$$L=L(u_1,\cdots,u_r)=L(v_1,\cdots,v_r).$$

即如 L 有一组基恰含 r 个线性无关的向量, 即 L 中任意 r 个线性无关的向量皆是 L 的一组基.

本定理为替换定理的直接推论.

定义 5　V_n 的一个非零子空间 L 的任一基中向量的个数称为 L 的维数. 零空间被认为以空集为基, 其维数定义为零.

系理　$L(u_1,\cdots,u_r)$ 的维数等于 $u_1,\cdots,u_r$ 中向量的线性无关最大数.

定理 7　设 L 和 M 为 V_n 的两个子空间, 其维数分别为 l 和 m, 而且 $L\subseteq M$, 则 $l\leqslant m$. 更进一步, 对于 L 的任何基, 我们都可以添上 M 中 $m-l$ 个元素使之成为 M 的一组基. 如果 $L\subseteq M$, 而且 $l=m$, 则 $L=M$.

本定理仍然是替换定理的直接推论.

§3 子空间的交和联

在本节中我们来研究 K 上的行空间 V_n. 我们定义两个子空间 L_1 和 L_2 的交 $L_1 \cap L_2$ 为 L_1 和 L_2 中公共向量之全体. 于是 $L_1 \cap L_2$ 亦是一个子空间. 包有 L_1 和 L_2 的最小子空间称为 L_1 和 L_2 的联, 记作 $L_1 \cup L_2$. 显然, $L_1 \cup L_2$ 由一切形为 $v_1 + v_2$ 的向量所组成, 其中 $v_1 \in L_1$ 而 $v_2 \in L_2$.

不难证明下列关于交和联的性质:

(1) $$L \cup L = L, \quad L \cap L = L;$$

(2) $$L_1 \cap L_2 = L_2 \cap L_1, \quad L_1 \cup L_2 = L_2 \cup L_1;$$

(3) $$L_1 \cap (L_2 \cap L_3) = (L_1 \cap L_2) \cap L_3,$$
$$L_1 \cup (L_2 \cup L_3) = (L_1 \cup L_2) \cup L_3;$$

(4) $$L_1 \cap (L_1 \cup L_2) = L_1, \quad L_1 \cup (L_1 \cap L_2) = L_1;$$

对于任意子空间 L, L_1, L_2 和 L_3.

如以 $d(L)$ 表子空间 L 的维数, 则有下述维数公式:

定理 1 设 L 和 M 为两子空间, 则

$$d(L) + d(M) = d(L \cup M) + d(L \cup M).$$

【证】 因为

$$L \cap M \subseteq L \subseteq V_n$$

和

$$L \cap M \subseteq M \subseteq V_n,$$

所以依定理 2.7 或直接依替换定理, 可以选取基元素使得

$$L \cap M = L(u_1, \cdots, u_s),$$
$$L = L(u_1, \cdots, u_s, v_1, \cdots, v_t),$$
$$M = L(u_1, \cdots, u_s, w_1, \cdots, w_q),$$

而 $u_1, \cdots, u_s, v_1, \cdots, v_t$ 线性无关, $u_1, \cdots, u_s, w_1, \cdots, w_q$ 线性无关. 如果我们能够证明

$$u_1, \cdots, u_s, v_1, \cdots, v_t, w_1, \cdots, w_q$$

线性无关, 则有

$$d(L \cup M) = s + t + q,$$

于是定理得证.

假定 $u_1, \cdots, u_s, v_1 \cdots, v_t, w_1, \cdots, w_q$ 线性相关, 则有 K 中元素 $a_1, \cdots, a_s, b_1 \cdots, b_t, c_1, \cdots, c_q$ 不全为 0, 使得

$$a_1 u_1 + \cdots + a_s u_s + b_1 v_1 + \cdots + b_t v_t + c_1 w_1 + \cdots + c_q w_q = 0.$$

因 $u_1, \cdots, u_s, v_1, \cdots, v_t$ 为 L 之基, 故 $c_1, \cdots, c_q$ 不全为 0; 同理, 因 $u_1, \cdots, u_s, w_1, \cdots, w_q$ 为 M 之基, 故 $b_1, \cdots, b_t$ 不全为 0. 可是向量

$$a_1 u_1 + \cdots + a_s u_s + b_1 v_1 + \cdots + b_t v_t = -(c_1 w_1 + \cdots + c_q w_q)$$

一方面不属于 $L \cap M$, 而另一方面又属于 L 和 M, 此为不可能, 因此 $u_1, \cdots, u_s, v_1, \cdots, v_t, w_1, \cdots, w_q$ 线性无关. 定理得证.

定理 2 如果 $L_1 \subseteq L_3$, 则

$$L_1 \cup (L_2 \cap L_3) = (L_1 \cup L_2) \cap L_3. \tag{5}$$

【证】 因为 $L_1 \subseteq L_3$ 及 $L_1 \subseteq L_1 \cup L_2$, 所以有

$$L_1 \subseteq (L_1 \cup L_2) \cap L_3.$$

因为

$$L_2 \cap L_3 \subseteq L_2 \subseteq L_1 \cup L_2 \quad 及 \quad L_2 \cap L_3 \subseteq L_3,$$

所以

$$L_2 \cap L_3 \subseteq (L_1 \cup L_2) \cap L_3.$$

将上列二式合并, 就有

$$L_1 \cup (L_2 \cap L_3) \subseteq (L_1 \cup L_2) \cap L_3.$$

因之, 依定理 2.7, 我们只要证明

$$d(L_1 \cup (L_2 \cap L_3)) = d((L_1 \cup L_2) \cap L_3)$$

就行了, 而这可以从定理 1 推出来. 实际上,

$$\begin{aligned} d(L_1 \cup (L_2 \cap L_3)) &= d(L_1) + d(L_2 \cap L_3) - d(L_1 \cap L_2 \cap L_3) \\ &= d(L_1) + d(L_2 \cap L_3) - d(L_1 \cap L_2) \quad (因 L_1 \subseteq L_3) \end{aligned}$$

$$\begin{aligned}&= d(L_1) + d(L_2) + d(L_3) - d(L_2 \cup L_3)\\ &\quad - [d(L_1) + d(L_2) - d(L_1 \cup L_2)]\\ &= d(L_3) + d(L_1 \cup L_2) - d[(L_1 \cup L_2) \cup L_3]\\ &= d((L_1 \cup L_2) \cap L_3).\end{aligned}$$

定理 3 对于任何子空间 L 都有子空间 M 存在, 使得

$$V_n = L \cup M,$$

而

$$L \cap M = 0.$$

(M 称为 L 的补空间.)

【证】 依定理 2.7, 我们可以选取

$$L = L(u_1, \cdots, u_r) \quad \text{及} \quad V_n = L(u_1, \cdots, u_n),$$

其中 $u_1, \cdots, u_n$ 线性无关. 于是

$$M = L(u_{r+1}, \cdots, u_n)$$

就适合定理所要求的性质.

定理 4 设 L 为 V_n 的子空间, 则对于任何单调递增而含于 L 的子空间序列:

$$L_0 \subset L_1 \subset L_2 \subset \cdots \subset L \quad (L_i \neq L_{i+1}),$$

都有一个整数 r 存在, 使得 $L_r = L$.

§4 子空间的矩阵表示, 矩阵的行秩

用矩阵来表示子空间这种方法是很方便的, 这在本书中将经常采用.

设 L 为 V_n 的子空间, 而 $u_1, \cdots, u_s$ 为 L 的一组生成元 (不一定是基), 即 $L = L(u_1, \cdots, u_s)$. 我们写出一个 $s \times n$ 矩阵

$$U = \begin{pmatrix} u_1 \\ \vdots \\ u_s \end{pmatrix},$$

并书 $L(U) = L(u_1, \cdots, u_s)$, 这就是说 $L(u_1, \cdots, u_s)$ 可以看作是由 U 的行向量所生成的 V_n 的子空间, 于是我们就说用矩阵 U 表示了子空间 L. U 称为对应于 L 的

一个矩阵. 显然这种表示法不是唯一的. 可是我们知道 U 的线性无关行向量的最大数等于 L 的维数, 而且 U 的行向量线性无关当且仅当 S 等于 $L(U)$ 的维数. 反之, 对于每个 $s\times n$ 矩阵 U, 我们都可以造一个由 U 的行向量 $u_1,\cdots,u_s$ 所生成的子空间 $L(u_1,\cdots,u_s)$. $L(u_1,\cdots,u_s)$ 称为对应于 U 的子空间. 从子空间的矩阵表示, 很自然地可以同时推出子空间及其对应的矩阵的性质来, 或从其中之一的性质推出另一的性质来.

首先, 我们将 §2 中线性相关的定义 (定义 2.1) 改述如下: s 个向量 $u_1,\cdots,u_s$ 线性相关, 当且仅当有一个 s 维向量 $b=(b_1,\cdots,b_s)\neq 0$ 存在, 使得

$$bU=0.$$

我们可以给出可逆矩阵的一个判断条件.

定理 1　一个 $n\times n$ 矩阵 A 可逆, 当且仅当 $L(A)=V_n$, 即 A 的行向量线性无关.

【证】　设 $L(A)=V_n$, 则 $I^{(n)}$ 的诸行向量可表成 A 的行向量的线性组合, 因而有 $n\times n$ 矩阵 B 存在, 使 $I^{(n)}=BA$. 将此式左乘以 A 得 $A=ABA$, 于是 $(I^{(n)}-AB)A=0$. 因 A 的行向量线性无关, 故 $I^{(n)}-AB=0$, 即 $I^{(n)}=AB$, 所以 A 可逆.

反之, 设 A 可逆, 即有 B 存在, 使 $BA=I^{(n)}$. 于是 $I^{(n)}$ 的行向量 (它们是 V_n 的一组基) 皆为 A 的行向量的线性组合, 因之, $V_n=L(I^{(n)})\subset L(A)$. 另一方面, 显然有 $L(A)\subset V_n$. 故 $L(A)=V_n$.

【备注】　我们定义一个 $n\times n$ 矩阵 A 为左可逆, 如有 B 存在, 使 $BA=I$, 而 B 称为 A 的一个左逆. 同样可定义 A 为右可逆及 A 的右逆. 在定理 1 的证明中, 实际上证明了, A 为左可逆当且仅当 A 为右可逆. 事实上, 设 A 左可逆, 依证明的第二部分有 $L(A)=V_n$, 再依证明的第一部分推出 A 亦右可逆. 反过来, 如 A 右可逆, 即有 B 存在, 使 $AB=I$, 则 B 左可逆, 依证明的第二部分有 $L(B)=V_n$, 再依证明的第一部分推出 $BA=I$, 即 A 左可逆.

设 A 左可逆 (或右可逆), 而 B 为 A 的一个左逆, C 为 A 的一个右逆, 则 $B=B(AC)=(BA)C=C$, 因之, A 只有一个左逆, 也只有一个右逆, 而它就是 A 的逆, 这时 A 是可逆矩阵.

现在我们给出下面这个重要的概念.

定义 1　一个矩阵的行秩为 r, 如 $L(U)$ 的维数是 r.

有了行秩的概念之后, 我们可以将定理 1 改述如下:

定理 2　一个 $n\times n$ 矩阵 A 可逆, 当且仅当 A 的行秩为 n.

下面的定理以后经常用到.

定理 3 设 A 为行秩 r 的 $m\times n$ 矩阵, 而 B 为行秩 n 的 $n\times l$ 矩阵, 则 AB 为行秩 r 的 $m\times l$ 矩阵.

【证】 设 A_1 为由 A 中删去某些行所得到的子矩阵, 并设 A_1 的型为 (s,n). 设 b 为 V_s 中向量, 则因 B 的行秩为 n, $bA_1B=0$ 当且仅当 $bA_1=0$. 因此 A 中线性无关行向量的最大数 r 亦为 AB 中线性无关行向量的最大数. 这就证明了本定理.

定理 4 设 A 为行秩 m 的 $m\times n$ 矩阵, 则 $m\leqslant n$, 而且有一个 $(n-m)\times n$ 的矩阵 B 存在, 使得 $\binom{A}{B}$ 可逆.

【证】 设 A 的行为 $u_1,\cdots,u_m$, 依假定, 它们线性无关, 因之 $m\leqslant n$. 依定理 2.7, 我们可以选取 V_n 的一组基为

$$u_1,\cdots,u_m,u_{m+1},\cdots,u_n.$$

令

$$B=\begin{pmatrix} u_{m+1}\\ \vdots\\ u_n\end{pmatrix},$$

则

$$\begin{pmatrix} A\\ B\end{pmatrix}=\begin{pmatrix} u_1\\ \vdots\\ u_n\end{pmatrix}$$

的行秩为 n, 因而可逆.

§5 基变换, 线性映射, 矩阵的等价

设 L 为 V_n 的一个 r 维子空间, 设

$$U=\begin{pmatrix} u_1\\ \vdots\\ u_r\end{pmatrix} \quad 及 \quad U^*=\begin{pmatrix} u_1^*\\ \vdots\\ u_r^*\end{pmatrix}$$

皆为行秩 r 的 $r\times n$ 矩阵, 而 $L(U)=L(U^*)=L$, 即 U 的行向量组成 L 的一组基, U^* 的行向量亦然. 因 U 的行向量组成 L 的一组基, 故 U^* 的行向量可表成 U 的诸行的线性组合, 即有 $r\times r$ 矩阵 P 存在, 使

$$U^*=PU. \tag{1}$$

同理有 $r\times r$ 矩阵 Q 存在, 使

$$U = QU^*. \tag{2}$$

将 (2) 代入 (1), 得

$$U^* = PQU^*.$$

因 U^* 的行向量线性无关, 故 $PQ = I$, 即 P, Q 皆可逆矩阵, 而 P, Q 互为逆矩阵.

反之, 设 U 为行秩 r 的 $r\times n$ 矩阵而 $L(U) = L$. 再设 P 为 $r\times r$ 可逆矩阵. 令

$$U^* = PU, \tag{1}$$

则

$$L(U^*) \subset L(U) = L. \tag{2}$$

依定理 4.3, U^* 的行秩亦为 r, 故 $L(U^*) = L(U)$. 因此 U^* 的诸行亦为 $L(U)$ 的一组基.

我们把 (1) 式, (2) 式称为 L 的基变换公式.

上面的讨论指明, 基变换系由可逆矩阵所实现, 而可逆矩阵可实现基变换. 这一事实至为重要.

现在设 U 为行秩 r 的 $r\times n$ 矩阵, 而 V 为行秩 s 的 $s\times n$ 矩阵. 我们来研究以下形状的方程:

$$\bar{U} = \begin{pmatrix} \bar{u}_1 \\ \vdots \\ \bar{u}_r \end{pmatrix} = AV, \tag{3}$$

而 A 为 $r\times s$ 矩阵. 显而易见 $\bar{u}_1, \cdots, \bar{u}_r \in L(V)$. 如令 $L(U)$ 中向量 $a_1u_1 + \cdots + a_ru_r$ 映到 $L(U)$ 中向量 $a_1\bar{u}_1 + \cdots + a_r\bar{u}_r$, 我们就得到从 $L(U)$ 到 $L(V)$ 之中的一个映射. 显然这个映射是线性映射, 即它具有性质:

I. 由 $u \to \bar{u}$ 及 $u' \to \bar{u}'$ 推出 $u + u' \to \bar{u} + \bar{u}'$;

II. 由 $u \to \bar{u}$ 推出 $au \to a\bar{u}$,

对于 $L(U)$ 中所有 u, u' 及 K 中所有 a. 因此, (3) 可看作给出从 $L(U)$ 到 $L(V)$ 之中的一个线性映射. 反之, 假定有一个从 $L(U)$ 到 $L(V)$ 的线性映射, 则这个映射可由 $u_1, \cdots, u_r$ 的像 $\bar{u}_1, \cdots, \bar{u}_r$ 完全确定. 将 $\bar{u}_1, \cdots, \bar{u}_r$ 用 V 的行向量表出就有

$$\bar{U} = \begin{pmatrix} \bar{u}_1 \\ \vdots \\ \bar{u}_r \end{pmatrix} = AV. \tag{3}$$

于是这个映射由 (3) 式完全确定. 由 V 的行线性无关, 故 A 是唯一确定的.

如果我们在 $L(U)$ 及 $L(V)$ 中选取新基, 而

$$U^* = PU, \quad V^* = QV$$

为基变换的公式, 其中 P 为 $r\times r$ 可逆矩阵, Q 为 $s\times s$ 可逆矩阵. 则对于新基而言, 线性映射 (3) 就采取以下形状:

$$\bar{U}^* = P\bar{U} = PAV = PAQ^{-1}V^*.$$

这建议下面的定义

定义 1 两个 $r\times s$ 矩阵 A 和 B 称为等价, 如果有两个型分别为 $r\times r$ 及 $s\times s$ 的可逆矩阵 P 和 Q 存在, 使

$$A = PBQ.$$

定理 1 在所有 $r\times s$ 矩阵组成的集合里, 矩阵的等价是一个等价关系, 即具有下列性质:

I. 对于所有 A, A 与 A 等价;

II. 如果 A 与 B 等价, 则 B 与 A 等价;

III. 如果 A 与 B 等价, B 与 C 等价, 则 A 与 C 等价.

【证】 我们有

(i) $A = I^{(r)}AI^{(s)}$;

(ii) 如果 $A = PBQ$, 则 $B = P^{-1}AQ^{-1}$;

(iii) 如果 $A = PBQ$, $B = RCS$, 则

$$A = (PR)C(SQ).$$

定理因而成立.

现在我们来求出 $r\times s$ 矩阵在等价之下的标准形, 换言之, 我们要求出一组形状简单的 $r\times s$ 矩阵, 具有性质:

(i) 它们之中任意两个皆不等价;

(ii) 任一 $r\times s$ 矩阵必与其中之一等价.

我们先证次之定理.

定理 2 等价矩阵的行秩相等.

【证】 设 A 和 B 为等价的 $r\times s$ 矩阵, 即有 $r\times r$ 可逆矩阵 P 及 $s\times s$ 可逆矩阵 Q 存在, 使

$$A = PBQ.$$

于是

$$P^{-1}A = BQ.$$

依定理 4.3, B 与 BQ 有相同的行秩; 又显然 A 与 $P^{-1}A$ 有相同的行秩. 因此 A 与 B 有相同的行秩.

定理 3　行秩为 p 的 $r \times s$ 矩阵必等价于

$$\begin{pmatrix} I^{(p)} & 0 \\ 0 & 0 \end{pmatrix}.$$

【证】　设 A 为行秩 p 的 $r \times s$ 矩阵. 一个 $r \times r$ 矩阵 P 称为置换矩阵, 如果它的每行及每列都只有一个 1 而有 $r-1$ 个 0, 易见 PA 就是由 A 经行的重新排列而得到的矩阵. 因 A 的行秩为 p, 故可取一置换矩阵 P 使 PA 的前 p 行线性无关, 而其余诸行是前 p 行的线性组合. 即

$$PA = \begin{pmatrix} u_1 \\ \vdots \\ u_n \end{pmatrix}, \quad u_i = \sum_{j=1}^{p} b_{ij} u_j \quad (p+1 \leqslant i \leqslant r).$$

令

$$B = (b_{ij})_{p+1 \leqslant i \leqslant r, 1 \leqslant j \leqslant p}$$

及

$$P_1 = \begin{pmatrix} I^{(p)} & 0 \\ -B & I^{(r-p)} \end{pmatrix},$$

则

$$P_1 P A = A_1,$$

而

$$A_1 = \begin{pmatrix} R \\ 0 \end{pmatrix},$$

其中 R 为 $p \times s$ 矩阵, 其行秩为 p. 依定理 4.4, 可得一 $s \times s$ 可逆矩阵

$$Q = \begin{pmatrix} R \\ D \end{pmatrix}.$$

因

$$A_1 = \begin{pmatrix} R \\ 0 \end{pmatrix} = \begin{pmatrix} I^{(p)} & 0 \\ 0 & 0 \end{pmatrix} \begin{pmatrix} R \\ D \end{pmatrix} = \begin{pmatrix} I^{(p)} & 0 \\ 0 & 0 \end{pmatrix} Q,$$

故

$$P_1PAQ^{-1} = \begin{pmatrix} I^{(p)} & 0 \\ 0 & 0 \end{pmatrix}.$$

定理证毕.

定理 2 和 3 凑在一起, 就回答了我们上面提出的问题.

§6 列空间及矩阵的秩

直到现在为止我们只讨论了行空间 (或左空间) 即所有 $1\times n$ 矩阵的集合, 并且把它作为我们研究矩阵的基础, 特别, 我们把 $m\times n$ 矩阵的行看作行向量. 与此相平行, 我们把一个 $n\times 1$ 矩阵看作一个 n 维列向量或右向量, 并定义一个列向量 u 与 K 中一元素 a 的乘积为 $n\times 1$ 矩阵 u 和 1×1 矩阵 a 的乘积 ua, 这样我们就得到了 n 维列空间 V_n', 此地"$'$"表示与行空间 V_n 相区别. 像在定义 2.1 中一样, 我们定义 m 个列向量 $u_1,\cdots,u_m$ 线性无关, 如果 K 中没有不全为零的元素 $a_1,\cdots,a_m$, 使得

$$u_1a_1+\cdots+u_ma_m=0.$$

然后我们可以得到 §2 ~ §5 中类似的结果.

特别, 我们定义一矩阵的列秩为其列所生成的 V_n' 的子空间的维数. 我们能够像 §5 中一样证明, 等价矩阵的列秩相等, 而且对每个列秩 p 的 $m\times n$ 矩阵 A, 都存在着 $m\times m$ 可逆矩阵 P 及 $n\times n$ 可逆矩阵 Q, 使

$$PAQ = \begin{pmatrix} I^{(p)} & 0 \\ 0 & 0 \end{pmatrix}.$$

这样我们就证明了

定理 1 对任何矩阵而言, 其行秩与列秩皆相等.

因此, 我们可以定义一矩阵之秩为其行秩.

今设 $A=(a_{ij})$ 为 $m\times n$ 矩阵, 我们定义 A 的转置矩阵 A' 为 $n\times m$ 矩阵

$$A'=(a_{ij}'),$$

而

$$a_{ij}'=a_{ji}\quad (i=1,2,\cdots,n;j=1,2,\cdots,m).$$

依定理 1, 我们知道 A' 的行秩等于 A' 的列秩. 如果 K 是域, 则行空间 V_n 和列空

间 V_n' 在下述意义下相重：存在一个一一映射, 使得由

$$(a_1, \cdots, a_n) \leftrightarrow \begin{pmatrix} a_1 \\ \vdots \\ a_n \end{pmatrix}$$

推出

$$a(a_1, \cdots, a_n) \leftrightarrow \begin{pmatrix} a_1 \\ \vdots \\ a_n \end{pmatrix} a$$

对 K 中任意元素 a 和 V_n 中任意向量 $(a_1, \cdots, a_n)$ 皆成立. 因之我们有

定理 2　设 K 为域, 则矩阵 A 之秩等于其转置矩阵的秩.

另一方面, 如果 K 不是域, 定理不一定成立. 因为这时 K 至少包有两个元素 a 和 b, 使得 $ab \neq ba$, 于是矩阵

$$A = \begin{pmatrix} 1 & a \\ b & ab \end{pmatrix}$$

的秩为 2, 而其转置矩阵之秩为 1.

关于矩阵之秩, 以下诸定理常常会用到.

定理 3　$m \times n$ 矩阵 A 的秩为 r 当且仅当 A 含有一个 (r, r) 型子矩阵其秩为 r, 而 A 没有秩大于 r 的子矩阵.

【证】　设 A 为秩为 r, 则 A 有 r 个线性无关的行, 而其余的行都线性相关于它们, 以 B 表由这 r 个线性无关的行所组成的子矩阵, B 为 $r \times n$ 矩阵而 B 之秩亦为 r, 因之 B 有 r 列线性无关, 以 C 表这 r 列所组成的矩阵, 则 C 为 $r \times r$ 矩阵而 C 之秩为 r.

设 A 有一子矩阵其秩 $s > r$, 则它含 s 个线性无关的行, 假定它们属于 A 的第 j_1 行, $\cdots$, 第 j_s 行, 则 A 的这些行亦线性无关, 因之 A 的秩 $\geqslant s > r$. 定理证毕.

定理 4　设 A 和 B 皆为 $m \times n$ 矩阵, 而其秩分别为 r_A 和 r_B, 则

$$r_{A+B} \leqslant r_A + r_B.$$

【证】　不失普遍性, 我们可以假定

$$A = \begin{pmatrix} I^{(r_A)} & 0 \\ 0 & 0 \end{pmatrix}.$$

令

$$B = \begin{pmatrix} B_1 \\ B_2 \end{pmatrix},$$

其中 B_1 为 (r_A, n) 型矩阵, B_2 为 $(m-r_A, n)$ 型矩阵, 则

$$r_{A+B} \leqslant \{(I^{(r_A)}0)+B_1\}\text{之秩}+B_2\text{之秩} \leqslant r_A+r_B.$$

定理 5 设 A 为 $l\times m$ 矩阵, B 为 $m\times n$ 矩阵, 而其秩分别为 r_A 和 r_B, 令 $C=AB$ 之秩为 r_C, 则

$$r_A+r_B-m \leqslant r_C \leqslant \min\{r_A, r_B\}.$$

【证】 (i) 因 B 之秩为 r_B, 故有 $m\times m$ 可逆矩阵 M 及 $n\times n$ 可逆矩阵 N 存在, 使

$$B=M\begin{pmatrix} I^{(r_B)} & 0 \\ 0 & 0 \end{pmatrix}N.$$

那么

$$C^*=CN^{-1},\quad A^*=AM$$

之秩仍分别为 r_C 和 r_A, 而

$$A^*\begin{pmatrix} I^{(r_B)} & 0 \\ 0 & 0 \end{pmatrix}=C^*.$$

因之, 只需研究矩阵 A^*, $\begin{pmatrix} I^{(r_B)} & 0 \\ 0 & 0 \end{pmatrix}$, 及 C^* 即可. 我们写

$$A^*=(A_1^*\ A_2^*),$$

其中 A_1^* 为 $l\times r_B$ 矩阵而 A_2^* 为 $l\times(m-r_B)$ 矩阵. 令 A^* 有 r_A 个线性无关的列, 故 A_1^* 至少有

$$r_A-(m-r_B)$$

个线性无关的列, 因之

$$C^*=A^*\begin{pmatrix} I^{(r_B)} & 0 \\ 0 & 0 \end{pmatrix}=(A_1^*\quad 0)$$

之秩 r_C 至少为

$$r_A+r_B-m.$$

(ii) 由方程 $C=AB$ 可知 C 的行线性相关于 B 的行, 因之 C 的行所生成之子空间属于 B 的行所生成之子空间, 所以

$$r_C \leqslant r_B.$$

同样, C 的列线性相关于 A 的列, 因之

$$r_C \leqslant r_A.$$

§7　齐次线性方程组

设 A 为 $m \times n$ 矩阵, 其系数属于 K. 考查适合方程

$$Au = 0 \tag{1}$$

的列向量, 这些列向量显然组成列空间 V_n' 的一个子空间. 今假定 A 之秩为 r, 则有两个型分别为 (m,m) 及 (n,n) 的可逆矩阵 P 和 Q 存在, 使得

$$PAQ = \begin{pmatrix} I^{(r)} & 0 \\ 0 & 0 \end{pmatrix}.$$

令 $w = Q^{-1}u$, 则

$$0 = PAu = PAQw, \tag{2}$$

因之, w 为如此一列向量, 其前 r 个分量为零, 而其余 $n-r$ 个分量可取任意值, 因此适合 (2) 的列向量 w 所组成的子空间的维数为 $n-r$, 于是适合 (1) 的列向量 u 所组成的子空间的维数亦为 $n-r$. 设 B 为表示此子空间之一矩阵, 则

$$AB = 0.$$

反之, 对于一个固定的秩为 $n-r$ 的 $n \times l$ 矩阵 B, 我们有一个 r 维的子空间, 此子空间由一矩阵 A 确定, 使

$$AB = 0.$$

因此, 在行空间 V_n 的子空间与列空间 V_n' 的子空间之间存在着一个对偶关系, 这个对偶关系可以描述如下:

对于 V_n 的每个 r 维的子空间 L 都对应着 V_n' 的一个 $n-r$ 维的子空间 R, 使得: 如以 A 和 B 分别表子空间 L 和 R 所对应的矩阵, 则

$$AB = 0,$$

而且反之亦然. 更进一步, 如果 L_1 和 L_2 是 V_n 的两个子空间, 而 R_1 和 R_2 是与它们相对应的 V_n' 的子空间, 则交 $L_1 \cap L_2$ 与联 $R_1 \cup R_2$ 相对应, 而联 $L_1 \cup L_2$ 与交 $R_1 \cap R_2$ 相对应.

§8 $GL_n(K)$ 的换位子群

以 $T_{ij}(\lambda)(i\neq j,\lambda\in K^*)$ 表 $GL_n(K)$ 中主对角线上的系数都是 $1,(i,j)$ 位置的系数是 λ 而其余位置的系数都是 0 的矩阵. 例如,

$$T_{12}(\lambda)=\begin{pmatrix}1&\lambda&0&\cdots&0\\0&1&0&\cdots&0\\0&0&1&\cdots&0\\\vdots&\vdots&&\ddots&\vdots\\0&0&0&\cdots&1\end{pmatrix}.$$

设 $M=(m_{ij})_{1\leqslant i,j\leqslant n}$ 为任意 $n\times n$ 矩阵, 则 $T_{ij}(\lambda)M$ 就是将 M 的第 i 行 $(m_{i1},\cdots,m_{in})$ 代入 $(m_{i1}+\lambda m_{j1},\cdots,m_{in}+\lambda m_{jn})$ 所得之矩阵, $MT_{ij}(\lambda)$ 就是将 M 的第 j 列 $(m_{1j},\cdots,m_{nj})$ 代入 $(m_{1j}+m_{1i}\lambda,\cdots,m_{nj}+m_{ni}\lambda)$ 所得之矩阵.

令

$$P_{ij}=T_{ij}(1)T_{ji}(-1)T_{ij}(1),$$

则 P_{ij} 就是主对角线上的系数除了 (i,i) 及 (j,j) 位置为 0 外, 其余位置都为 $1,(i,j)$ 位置系数为 $1,(j,i)$ 位置系数为 -1, 而其余位置系数都是 0 的矩阵. 例如,

$$P_{12}=\begin{pmatrix}0&1&0&\cdots&0\\-1&0&0&\cdots&0\\0&0&1&\cdots&0\\\vdots&\vdots&\vdots&\ddots&\vdots\\0&0&0&\cdots&1\end{pmatrix}.$$

显然, $P_{ij}M$ 就是将 M 的第 i 行和第 j 行互换, 然后再将第 j 行乘以 -1 所得到的矩阵. MP_{ij} 就是将 M 的第 i 列和第 j 列互换, 然后再将第 i 列乘以 -1 所得到的矩阵.

所有 $T_{ij}(\lambda)$ 对所有 i 和 j, 而 $i\neq j$ 及所有 $\lambda\in K^*$, 所生成的群, 称为 K 上 n 级特殊线性群, 记作 $SL_n(K)$.

定理 1 任何 $n\times n$ 可逆矩阵 A 皆可表作

$$A=BD(\mu),$$

其中 $B\in SL_n(K)$ 而 $D(\mu)=[1,\cdots,1,\mu]$ 为对角形矩阵, $\mu\neq 0$.

【证】 设 $A=(a_{ij})$ 为 $n\times n$ 可逆矩阵. A 的第一列中至少有一个元素 $\neq 0$, 将 A 左乘以一个适当的 P_{ij} 之后, 可以假定 $a_{21}\neq 0$. 再将 A 左乘以一个适当的

$T_{12}(\lambda)$ 之后, 我们就得到一个矩阵 $B=(b_{ij})$ 而 $b_{11}=1$. 将 B 的第一行的适当的左倍数加到其余诸行就可以得到一个矩阵 $C=(c_{ij})$, 而 $c_{11}=1, c_{i1}=0(i\neq 1)$. 因为 A 可逆, 所以 (c_{ij}) 的第二列中有一个元素 $c_{i2}\neq 0(i\neq 1)$. 如果 $n>2$, 将 C 左乘以一个适当的 P_{ij} 之后, 可以假定 $c_{32}\neq 0$. 再将 C 左乘以一个适当的 $T_{23}(\lambda)$ 之后我们就得到一个矩阵 $D=(d_{ij})$, 其第一列与 C 的第一列一样, 而其 (2,2) 位置元素为 1. 用同样的办法, 我们可以使 $d_{i2}=0(i\neq 2)$. 这样一步步地下去就得到一个矩阵

$$\begin{pmatrix} 1 & 0 & \cdots & 0 & \lambda_{1n} \\ 0 & 1 & \cdots & 0 & \lambda_{2n} \\ \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & 0 & \cdots & 1 & \lambda_{n-1,\,n} \\ 0 & 0 & \cdots & 0 & \lambda_{nn} \end{pmatrix}.$$

因 A 可逆, 故 $\lambda_{nn}\neq 0$; 将这个矩阵的最后一行的适当的左倍数加到其余各行就得到一个矩阵 $D(\mu)$, 而 $\mu\neq 0$.

定理 2 $SL_n(K)$ 是 $GL_n(K)$ 的正规子群.

【证】 依定理 1, 只须证 $SL_n(K)$ 在 $D(\mu)$ 之下不变, 而 μ 为 K 中任意非零元素. 因为

$$\begin{aligned} D(\mu)T_{ij}(\lambda)D(\mu)^{-1} &= T_{ij}(\lambda) \quad (\text{若} i\neq n, j\neq n), \\ D(\mu)T_{in}(\lambda)D(\mu)^{-1} &= T_{in}(\lambda\mu^{-1}), \\ D(\mu)T_{nj}(\lambda)D(\mu)^{-1} &= T_{nj}(\mu\lambda), \end{aligned}$$

所以本定理成立.

最后我们证明

定理 3 设 $n\geqslant 2$, 则 $GL_n(K)$ 的换位子群一定包在 $SL_n(K)$ 中; 更进一步, 除开 $n=2$ 而 $K=F_2$ 外, $SL_n(K)$ 即是 $GL_n(K)$ 的换位子群.

【证】 设 $\mathfrak{C}_n$ 是 $GL_n(K)$ 的换位子群. 设 A 和 A_1 为 $GL_n(K)$ 中任意二元素, 依定理 1, 有

$$A=BD(\mu), \quad A_1=B_1D(\mu_1),$$

而 $B, B_1\in SL_n(K)$. 于是

$$\begin{aligned} AA_1A^{-1}A_1^{-1}SL_n(K) &= D(\mu)D(\mu_1)D(\mu)^{-1}D(\mu_1)^{-1}SL_n(K) \\ &= D(\mu\mu_1\mu_1^{-1}\mu_1^{-1})SL_n(K). \end{aligned}$$

由第二章 §4(2), (3), (4) 式知 $D(\mu\mu_1\mu^{-1}\mu_1^{-1})\in SL_n(K)$, 故 A 和 A_1 的换位子 $AA_1A^{-1}A_1^{-1}$ 属于 $SL_n(K)$. 因之 $\mathfrak{C}_n\subseteq SL_n(K)$. 这证明了本定理的第一个断言.

现在来证明第二个断言. $n=2$ 的情形在第二章 §4 中已经讨论过了, 我们现在假定 $n \geqslant 3$. 由

$$\begin{pmatrix} 1 & 0 & 0 \\ 1 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix} = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 1 \\ 0 & 0 & 1 \end{pmatrix} \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 1 & 0 & 1 \end{pmatrix} \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 1 \\ 0 & 0 & 1 \end{pmatrix}^{-1} \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 1 & 0 & 1 \end{pmatrix}^{-1}$$

推知 $T_{21}(1) \in \mathfrak{C}_n$. 因 $\mathfrak{C}_n$ 为 $GL_n(K)$ 的正规子群, 所以 $\mathfrak{C}_n$ 亦包有

$$T_{21}(\lambda) = [1, \lambda, 1, \cdots, 1] T_{21}(1) [1, \lambda, 1, \cdots, 1]^{-1}$$

对任意 $\lambda \in K^*$, 其中 $[1, \lambda, 1, \cdots, 1]$ 表主对角线上元素依序为 $1, \lambda, 1, \cdots, 1$ 的对角形矩阵. 因而 $\mathfrak{C}_n$ 亦包有

$$\begin{aligned} T_{i1}(\lambda) &= P_{2i}^{-1} T_{21}(\lambda) P_{2t} \quad (i \neq 2), \\ T_{ij}(\lambda) &= P_{1j}^{-1} T_{i1}(\lambda) P_{1j} \quad (j \neq 1, i), \\ T_{1j}(\lambda) &= P_{1i}^{-1} T_{ij}(\lambda) P_{1i}, \end{aligned}$$

所以 $T_{ij}(\lambda) \in \mathfrak{C}_n$, 对于所有 i 和 $j (i \neq j)$ 及所有 $\lambda \in K^*$. 这就证明了

$$SL_n(K) \subseteq \mathfrak{C}_n.$$

因此

$$\mathfrak{C}_n = SL_n(K).$$

§9 行 列 式

如 K 为域, 我们有熟知的行列式理论. 以 $\det A$ 表 $n \times n$ 矩阵 A 的行列式, 我们知道有行列式的乘性:

$$\det AB = \det A \det B,$$

特别, 如 $A \in GL_n(K)$, 则

$$A \to \det A$$

是从 $GL_n(K)$ 到 K 的乘法群 K^* 之上的一个同态映射. 这个同态的核记作 $\mathfrak{N}$, 则 $\mathfrak{N}$ 由 $GL_n(K)$ 中行列式为 1 的矩阵组成. 显然有 $\det T_{ij}(\lambda) = 1$, 因之, $\det B = 1$ 对一切 $B \in SL_n(K)$, 换言之, $SL_n(K) \subset \mathfrak{N}$. 根据定理 8.1, $GL_n(K)$ 中任一矩阵 A 皆可表作

$$A = BD(\mu),$$

其中 $B \in SL_n(K)$ 而 $D(\mu)$ 为对角矩阵 $[1,1,\cdots,1,\mu]$. 于是 $\det A=\mu$, 因之, $\det A=1$ 当且仅当 $\mu=1$, 所以

$$SL_n(K)=\mathfrak{N}.$$

这样, 当 K 为域时, 我们就利用行列式给出了刻画 $SL_n(K)$ 的一个方法, 即 $SL_n(K)$ 由 $GL_n(K)$ 中所有行列式为 1 的矩阵组成.

当 K 为体时, 我们希望有类似的刻画 $SL_n(K)$ 的方法, 为此我们将行列式推广到体上来, 而使体上的行列式仍具有行列式的乘性, 同时 $SL_n(K)$ 仍为 $GL_n(K)$ 中所有行列式为 1 的矩阵组成. 我们知道, 当 μ 为 K^* 中换位子时, $D(\mu)$ 属于 $SL_n(K)$; 因此就建议我们这时行列式取值的范围不再是 K^* 而是商群 K^*/C. 以

$$a \to \varphi(a)$$

表由 K^* 到 K^*/C 之上的自然同态映射, C 为 K^* 的换位子群. 我们用归纳法来定义行列式如下:

设 $A=(a_{ij})_{1\leqslant i,j\leqslant n}$ 为 $GL_n(K)$ 中任意元素, 而 $n>1$, A 的第一列中至少有一个元素 $\neq 0$; 设 $a_{i1}\neq 0$, 将 A 的第 i 行的适当左倍数加到其余各行, 可以得到一个矩阵 $(a'_{ij})_{1\leqslant i,j\leqslant n}$, 其中 $a'_{i1}=a_{i1}$, 而 $a'_{j1}=0\ (j\neq i)$. 以 A_{n-1} 表由 (a'_{ij}) 中删去第一列及第 i 行后所得到的子矩阵, 定义

$$\det A=\varphi((-1)^{i+1}a_{i1})\ \det(A_{n-1}).$$

我们首先需要证明:

I. $\det A$ 与 A 的第一列中元素 a_{i1} 的选取无关.

我们用归纳法来证明 I, 在证明它的同时, 我们还要证明以下两点:

II. 如果我们将 A 的某一行加上另一行的一个左倍数, 则 $\det A$ 不变.

III. 如果将 A 的某一行左乘以 K^* 中一个元素 μ, 则 $\det A$ 就变成了 $\varphi(\mu)\det A$.

现在假设 I, II, III 对 $n-1$ 成立, 我们来证明它们对 n 亦成立. 为简单起见, 我们只写出 $n=3$ 的证明, 但可看出证明的方法对一般情形也成立.

设

$$A=\begin{pmatrix} a_1 & b_1 & c_1 \\ a_2 & b_2 & c_2 \\ a_3 & b_3 & c_3 \end{pmatrix}$$

假定 $a_1\neq 0$ 和 $a_2\neq 0$. 由 a_1 得到的 A_2 为

$$A_2(a_1)=\begin{pmatrix} b_2-a_2a_1^{-1}b_1 & c_2-a_2a_1^{-1}c_1 \\ b_3-a_3a_1^{-1}b_1 & c_3-a_3a_1^{-1}c_1 \end{pmatrix},$$

于是

$$\det A=\varphi(a_1)\det(A_2(a_1)).$$

另一方面, 用由 a_2 所得的 A_2 来定义 $\det A$, 就有

$$\det A=\varphi(-a_2)\det(A_2(a_2)),$$

由

$$A_2(a_2)=\begin{pmatrix} b_1-a_1a_2^{-1}b_2 & c_1-a_1a_2^{-1}c_2 \\ b_3-a_3a_2^{-1}b_2 & c_3-a_3a_2^{-1}c_2 \end{pmatrix}.$$

可将 $A_2(a_2)$ 改写成

$$A_2(a_2)=\begin{pmatrix} -a_1a_2^{-1}(b_2-a_2a_1^{-1}b_1) & -a_1a_2^{-1}(c_2-a_2a_1^{-1}c_1) \\ (b_3-a_3a_1^{-1}b_1)-a_3a_2^{-1}(b_2-a_2a_1^{-1}b_1) & (c_3-a_3a_1^{-1}c_1)-a_3a_2^{-1}(c_2-a_2a_1^{-1}c_1) \end{pmatrix}.$$

可见 $A_2(a_2)$ 可由 $A_2(a_1)$ 经将第二行加以第一行的 $(-a_3a_2^{-1})$ 倍并将第一行左乘以 $(-a_1a_2^{-1})$ 倍而得到. 依 $n=2$ 时的 II 和 III 就有

$$\det(A_2(a_2))=\varphi(-a_1a_2^{-1})\det(A_2(a_1)),$$

由于

$$\varphi(-a_1a_2^{-1})=\varphi(a_1)\varphi(-a_2)^{-1},$$

因之, I 对于 $n=3$ 亦成立.

现在来证明 II 对 $n=3$ 亦成立. 为确定起见, 假定 $a_1\neq 0$. 今有

$$b_2+\lambda b_1-(a_2+\lambda a_1)a_1^{-1}b_1=b_2-a_2a_1^{-1}b_1,$$

所以如果我们将第一行的某个左倍数加到足码 $\neq 1$ 的一行上去, 矩阵 $A_2(a_1)$ 不变, 因之, $\det A$ 不变. 如果我们将足码 $j\neq 1$ 的一行的某个左倍数加到足码 $\neq 1$ 的另一行去, $A_2(a_1)$ 亦经受同样的变化, 依 $n=2$ 的 II 可知 $\det(A_2(a_1))$ 不变, 因之, $\det A$ 亦不变. 最后, 假如我们将第一行加上另一行的一个左倍数, 如 $a_2=a_3=0$, 则 a_1 和矩阵 $A_2(a_1)$ 在此变换下不变, 因此 $\det A$ 不变; 如 $a_2\neq 0$ 或 $a_3\neq 0$, 只须用 a_2 或 a_3 来代替 a_1 以计算 $\det A$, 则根据前面结果 $\det A$ 亦不变. 因此 II 得证.

最后, 我们将 A 的第一行左乘以 μ, 则 a_1 被 μa_1 所代替, 而 $A_2(a_1)$ 不变, 因之 $\det A$ 就变成了 $\varphi(\mu)\det A$. 如果我们将任意另外一行左乘以 μ, 则 a_1 不变, 而 $A_2(a_1)$ 的相应一行亦左乘上了 μ, 因之 $\det A$ 亦变到了 $\varphi(\mu)\det A$. 所以 III 得证.

这样我们就证明了

(1) $$A\to\det A$$

是从 $GL_n(K)$ 到 K^*/C 之中的一个映射. 更进一步有

定理 1　设 K 为体, 而 $n>1$, 则如上所定义的映射 (1) 是从 $GL_n(K)$ 到 K^*/C 之上的一个同态, 而且这个同态的核为 $SL_n(K)$, 即

$$GL_n(K)/SL_n(K)\cong K^*/C.$$

【证】　依定理 8.1, $GL_n(K)$ 中任一矩阵 A 皆可表作

$$A=BD(\mu),$$

其中 $B\in SL_n(K)$. 依 II 有

$$\det A=\det(D(\mu)).$$

再依行列式的定义, 显然有

$$\det A=\varphi(\mu).$$

由此立刻推出 (1) 是映上的.

再者, 设 A 和 A_1 是 $GL_n(K)$ 中两个元素, 表

$$A=BD(\lambda),\quad A_1=B_1D(\mu),$$

其中 $B,B_1\in SL_n(K)$, 则

$$\begin{aligned}\det AA_1&=\det BD(\lambda)A_1=\det D(\lambda)A_1=\varphi(\lambda)\det B_1D(\mu)\\&=\varphi(\lambda)\det D(\mu)=\varphi(\lambda)\varphi(\mu)\\&=\det A\,\det A_1.\end{aligned}$$

这就证明了 (1) 是同态.

最后, 设 $A=BD(\mu)\in GL_n(K)$ 而 $B\in SL_n(K)$. 则 $\det A=\varphi(\mu)$. 因此 $\det A=C$ 当且仅当 $\mu\in C$, 即当且仅当 $A\in SL_n(K)$. 于是 $SL_n(K)$ 是同态映射 (1) 的核.

至此, 定理 1 完全证毕.

我们再次指出, 基于定理 1, 映射 (1) 给出了刻画 $SL_n(K)$ 的一个方法.

上面, 我们对于 $GL_n(K)$ 中的元素 A 都定义了 $\det A$, 而且我们知道它是 Abel 群 K^*/C 中的一个元素. 对于不可逆的 A, 我们规定 $\det A=0$, 而 0 是一个添加到 K^*/C 上去的元素, 并约定 $0\cdot\sigma=\sigma\cdot 0=0$ 对一切 $\sigma\in K^*/C$ 及 $0\cdot 0=0$. 这样, 对于任意两个 $n\times n$ 矩阵 A 和 A_1, 我们都有

$$\det AA_1=\det A\,\det A_1.$$

我们就把上面定义的 $\det A$(A 可逆或不可逆) 称为 A 的行列式.

当 K 为域时, C 就化为 K 的单位元素组成的群. 这时, 我们可以将群 K^*/C 就看作是 K^*, 而将另外添加的元素 0 看作是 K 中零元素. 于是 $\det A$ 总是 K 中一个元素, 这时我们所定义的行列式与通常的行列式相符. 然而, 当 K 不是域时, 我们尚不能断言 K^*/C 是否与 K^* 的一个子群同构, 因而不能断言 $\det A$ 是否可看作 K 中元素. 但下面王湘浩的例子指明, Abel 群 K^*/C 不能和 K^* 的中心 Z^* 的一个子群同构.

设 D 为 F_2 上的全体形式幂级数

$$\sum_{\gamma=r}^{\infty} a_\gamma x^\gamma \quad (a_\gamma = 0\text{或}1, r \gtreqless 0)$$

所组成的域. 引进一个新的未定元 y, 而考查 D 上的形式幂级数

$$\sum_{\mu=s}^{\infty} a_\mu y^\mu \quad (a_\mu \in D, s \gtreqless 0).$$

我们形式地定义 D 上两个形式幂级数相加为将相应系数相加, 而根据规则 $y\alpha = \alpha^\sigma y (\alpha \in D)$, 来形式地定义 D 上两个形式幂级数相乘, 这里 σ 是 D 的一个自同构, 它由方程

$$x^\sigma = x + x^2$$

所定义. 易证, 这样定义了加法和乘法之后, D 上全体形式幂级数组成一体, 记作 K. 注意 D 中在 σ 之下不变的元素只有 F_2 中的元素, 因此 K 的中心 $Z = F_2$. 另一方面, 设 $\xi = \sum_{\mu=s}^{\infty} a_\mu y^\mu \in K$, 而 $a_s \neq 0$. 定义 $|\xi| = y^s$, 依乘法规则 $|\xi\eta| = |\xi||\eta|$, 这表明

$$\xi \to |\xi|$$

是从 K^* 到由 y 生成的无限循环群 $\{y\}$ 的一个同态, 因 $\{y\}$ 是 Abel 群, 所以它是 K^*/C 的一个同态像. 这时 $Z = \{1\}$, 故 K^*/C 不可能与 Z^* 的子群同构.

现在我们来证明关于行列式的一些常用的性质.

IV. 如将 A 之两行互换, 则 $\det A$ 就变成 $\varphi(-1)\det A$.

这个断言是下列等式的推论:

$$\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}.$$

V. 对于列而言, 我们有以下类似的性质:

V.1. 如果将 A 的某一列右乘以 K^* 中一元素 μ, 则 $\det A$ 就变成 $\varphi(\mu)\det A$.

V.2. 如果将 A 的某一列加上另一列的一个右倍数, 则 $\det A$ 不变.

V.3. 如果将 A 的某两列互换, 则 $\det A$ 就变成了 $\varphi(-1)\det A$.

这三个断言的证明有赖于 $SL_n(K)$ 是 $GL_n(K)$ 的正规子群这一事实. 因对于任意 $B \in SL_n(K)$, 我们可以写

$$BD(\mu) = D(\mu)B',$$

而 $B' \in SL_n(K)$. 我们再指出, 如利用将 A 右乘以 $T_{ij}(\lambda)$ 引起 A 的列变化的方法亦可定义 $\det A$, 而这两个定义显然是等价的.

VI. 如 A 为 $m \times m$ 矩阵, D 为 $(n-m)\times(n-m)$ 矩阵, 则

$$\det\begin{pmatrix} A & B \\ 0 & D \end{pmatrix} = \det A \det D.$$

证明略去.

VII. 如果 A 为 $m \times m$ 可逆矩阵, 则

$$\det\begin{pmatrix} A & B \\ C & D \end{pmatrix} = \det A \det(D - CA^{-1}B).$$

这是下式的推论.

$$\begin{pmatrix} I^{(m)} & 0 \\ -CA^{-1} & I^{(n-m)} \end{pmatrix}\begin{pmatrix} A & B \\ C & D \end{pmatrix} = \begin{pmatrix} A & B \\ 0 & D - CA^{-1}B \end{pmatrix}.$$

VIII. 对于可逆矩阵 X, 恒有

$$\det A = \det(XAX^{-1}).$$

一般地, 如 λ 为 K 的一个中心元素, 而 X 为可逆矩阵, 则

$$\det(\lambda I - A) = \det(\lambda I - XAX^{-1}).$$

IX. Cramér 规则. 设 $A = (a_{ij})_{1\leqslant i,j\leqslant n}$ 为可逆矩阵, 研究方程组

$$\sum_{j=1}^{n} a_{ij}x_j = b_i \quad (1 \leqslant i \leqslant n). \tag{2}$$

以 A_i 表将 A 的第 i 列代之以 $(b_1, \cdots, b_n)'$ 所得之矩阵: 设 $x_1, x_2, \cdots, x_n$ 为 (2) 的解, 如 $x_i \neq 0$ 则

$$\det A_i = \varphi(x_i)\det A. \tag{3}$$

如果 $x_i=0$, 而 $\det A_i=0$.

实际上, 如 $x_i\neq 0$, 则

$$A_i=\begin{pmatrix} a_{11}\cdots a_{1,i-1} & a_{11}x_1+\cdots+a_{1n}x_n & a_{1,i+1}\cdots a_{1n}\\ \cdots\cdots & \cdots\cdots & \cdots\cdots\\ a_{n1}\cdots a_{n,i-1} & a_{n1}x_1+\cdots+a_{nn}x_n & a_{n,i+1}\cdots a_{nn}\end{pmatrix}$$

可逆, 于是 (3) 式可从 V.1 及 V.2 推出. 如 $x_i=0$, 则 A_i 不可逆, 因此 $\det A_i=0$.

特别, 当 K 为域时, 我们有

$$x_i=\frac{\det A_i}{\det A}.$$

最后, 我们指出, 从以上的讨论可知, 研究 K^* 的换位子群是个很重要的问题. 当 $C=K^*$ 时, 上面关于行列式的定义就失去意义. 但目前我们关于体的知识尚不能给出 $C=K^*$ 的例子. 如果 K 在其中心 Z 上是有限维的, 我们知道 $C=K^*$ 不可能成立. 实际上, 设 $e_1,e_2,\cdots,e_m$ 是 K 在 Z 上的一组基, 如 $\lambda\in K$, 令

$$\lambda e_j=\sum_{i=1}^{m}a_{ij}e_j\quad(1\leqslant j\leqslant m),$$

而 $a_{ij}\in Z$. 定义

$$N(\lambda)=\det(a_{ij}),$$

我们称 $N(\lambda)$ 为 λ 对于 Z 的范. 易证, 如 $\lambda,\mu\in K$, 则

$$N(\lambda\mu)=N(\lambda)N(\mu),$$

而且 $N(\lambda)=0$ 当且仅当 $\lambda=0$. 因此, 如 $\lambda\in K^*$, 则

$$\lambda\to N(\lambda)\tag{4}$$

是从 K^* 到 Z^* 之中的一个同态映射. 对于 $a\in Z^*$, 显然有 $N(a)=a^m$. 因为 K 不是域, Z 不可能是有限域, 所以一定有一个 $a\in Z^*$ 使 $a^m\neq 1$. 因此映射 (4) 的像不可能仅含一个元素. 又因为映射 (4) 的像是个 Abel 群, 因而与 K^*/C 的一个商群同构, 所以 $C\neq K^*$.

一个自然发生的问题是何时映射 (4) 的像与 K^*/C 同构, 即何时 C 与 K 中范为 1 的元素所组成的群相重. 当 K 为实四元数体 (或一般地, 一个有序毕氏域上的四元数体) 时, 情况的确是这样的. 这时范为 1 的元素不仅属于 C, 而且可以表成换位子. 实际上, 设 K 为其中心毕氏域 Z 上的四元数体, 而 $\lambda=a_0+a_1i+a_2j+a_3k\in K$, 则

$$N(\lambda)=(a_0^2+a_1^2+a_2^2+a_3^2)^2.$$

设 $N(\lambda)=1$, 即 $a_0^2+a_1^2+a_2^2+a_3^2=1$. 如 $\lambda=\pm1$, 则 1 显然为换位子而 $-1=iji^{-1}j^{-1}$ 亦为换位子. 如 $\lambda\neq\pm1$, 则 $x\notin Z$, 因之 $Z(\lambda)$ 是 Z 的一个二次扩域. 因 Z 为有序毕氏域, $Z(\lambda)$ 中任一元素在其中皆有平方根, 特别有 $\mu\in Z(\lambda)$, 使 $\mu^2=\lambda$. 因 $N(\lambda)=1$, 故 $N(\mu)=1$. 因此 $\mu^{-1}=\bar{\mu}$. 又因 μ 和 $\bar{\mu}$ 有相同的范和迹, 故有 $\alpha\in K$, 使 $a^{-1}\mu\alpha=\bar{\mu}$. 因此 $\lambda=\mu\alpha\mu^{-1}\alpha^{-1}$ 为换位子. (注意, 在证明中, 我们还可以取 $N(\alpha)=1$, 因此我们还证明了范为 1 的元素皆范为 1 的元素的换位子.)

第四章　射影几何与仿射几何

§1　几 何 结 构

人们对于几何学有许多种观点, 以下这种观点对于本书而言是方便的.

设 S 为一集合, 其上有一个变换群 G 作用着. S 称为空间, 而 S 中的个别元素则称为点. G 称为 S 的运动群或变换群, 而 G 中的个别元素则称为运动或变换. S 的任何子集皆称为图形. 两个图形称为等价或合同, 如果有一个 G 中的变换将其中之一变到其中的另一个. 因为 G 是群, 故这是个等价关系. 因之, S 中图形就分成等价图形类, 属于同一类的图形的任何共同性质都称为 G 的一个不变量. F·Klein 在他著名的爱兰根纲领中将几何学定义如下:

"表述空间中图形在一已知变换群之下不变的性质的定义和定理的系统称为几何学". 换言之, 几何学就是研究图形在空间的变换群之下不变的性质的 (由定义和定理所表达出来的) 学问, 或研究变换群的不变量理论的学问.

设 H 为 G 之子群, 则 S 在 G 之下的不变量也在 H 之下不变, 可是, 能有在 H 之下的不变量却并不在 G 之下不变. 因之, 群越小, 空间就越复杂. 一个极端情形就是群由单位变换组成, 这时几何学最大; 另一极端情形就是群由 S 中所有变换组成, 这时几何学最小. 这两个情形的趣味都不大.

为了说明上述原理, 我们举出以下诸例:

〔**例 1**〕　S 由四个文字 1, 2, 3, 4 所组成. 设 S_4, A_4, V_4 分别表对称群, 交错群, 肆群, 于是我们就得到空间 S 的三种几何学. 算式

$$\prod_{1\leqslant i<j\leqslant 4}(x_i-x_j)$$

为 A_4 的不变量, 但却不是 S_4 的不变量; 而算式

$$x_1x_2+x_3x_4$$

为 V_4 的不变量, 但却不是 A_4 的不变量.

这个例子建议整个的 Galois 理论可以几何地加以研究.

〔**例 2**〕　设 S 为群, G 为 S 的自同构群, 则 S 的特性子群都在 G 之下不变. 如果, H 是内自同构群, 则 S 的正规子群都在 H 之下不变.

〔例 3〕　设 S 为平面上的点集, G 为刚体运动群, 则两点 (x_1, y_1) 和 (x_2, y_2) 之间的距离

$$\sqrt{(x_1 - x_2)^2 + (y_1 - y_2)^2}$$

为一不变量.

〔例 4〕　设 S 为 $r \times s$ 矩阵的集合, G 为矩阵的等价群, 则"秩"为一不变量.

〔例 5〕　设 $f(x)$ 为定义在 $-\infty < x < \infty$ 上的函数, S 为使积分

$$\int_{-\infty}^{\infty} |f(x)|^2 \mathrm{d}x$$

收敛的函数 $f(x)$ 的全体, 即 $S = L^2$. 以 G 表变换

$$g(y) = \int_{-\infty}^{\infty} f(x) e^{2\pi i x y} \mathrm{d}x$$

所成之集合, Fourier 积分理论中证明 G 将 S 变到它自己上面, 而函数

$$||f(x)|| = \int_{-\infty}^{\infty} |f(x)|^2 \mathrm{d}x$$

为一不变量.

为了研究方便起见, 我们常在空间中引进坐标. 空间 S 中的一个"坐标系"就是由 S 到数组集合的一个子集的一个单价映射 $p \to (x)$. 如此, S 的每个点 p 都用一个数组 (x) 表了出来. 这个映射, 并不要求是单值的. 表示点 p 的任何一个数组 (x) 都称为 p 的坐标.

今假定我们有一个具变换群 G 的空间 S. 假定在 S 中已经引入了坐标, 则表 S 中点的数组就称为组成一个数量空间 $\bar{S}$. 如果以 π 表空间 S 的变换群 G 中的一个元素, 则可以确定 $\bar{S}$ 中的一个变换 $\bar{\pi}$ 如下:

$$(x)\bar{\pi} = (x)\tau^{-1}\pi\tau,$$

而其中 τ 表映射 $p \to (x)$. 所有变换 $\bar{\pi}$ 的集合组成一群 $\bar{G}$ 与 G 同构. 如果 $p \to (x)$ 为 S 的一个坐标系, 则 $p \to (x)\bar{\pi}$ 也为 S 的一个坐标系, 其中 $\bar{\pi}$ 为 $\bar{G}$ 中任意元素. 如此得到的 S 的坐标系称为可许坐标系. 显然, S 的性质为 G 所不变当且仅当它在每个可许坐标系中都有此性质.

S 中两点称为在 G 之下可迁, 如果 G 中有一变换将其中之一变到其中之另一个, 即它们在 G 之下等价. 在此等价关系下, S 中元素分到一些等价类里, 每一个等价类称为一个可迁系. 如果 S 只有一个可迁系, 则 S 称为可迁的. 例如, 例 1 中的空间在 S_4, A_4, V_4 之下都是可迁的, 而例 4 的空间却不是可迁的. 在一可迁空间中, 将一固定点不变的变换所组成的子群称为稳定群.

几何学中深入之问题为求出基本不变量系的问题. 所谓基本不变量系, 即为能完全确定出空间 S 的变换群 G 的不变量系, 换言之, G 为 S 中所有变换所组成的群中将这组不变量不变的最大子群. 例如实数域的自同构群由单位变换组成, 即所有实数所组成的域到它自己的一一变换如果保持加性或乘性不变, 则为单位变换, 因之, 加性和乘性为全体实数所组成的空间在自同构群之下的一组基本不变量.

今假定我们有具变换群 G 的空间 S. 设 P 为 S 的一个性质, 并假定这个性质并不在 G 之下不变. 令 H 为 G 的使 P 不变的最大的子群, 则我们可以研究空间 S 与群 H 的几何学. 这个几何学通常称之为由绝对 P 所诱导出来的几何. 例如, 设 S 为复平面, G 为 Möbius 群, 其中元素为 Möbius 变换:

$$Z' = (az+b)(cz+d)^{-1} \quad (ad-bc \neq 0).$$

取单位圆

$$|z| = 1$$

为绝对, 则 G 中使 $|z|=1$ 不变的子群 H 中之变换为下列形状:

$$Z' = (az+b)(\bar{b}z+\bar{a})^{-1} \quad (a\bar{a}-b\bar{b}=1).$$

我们得到 S 在群 H 之下的几何学. 这个几何学的空间不是可迁的, 它由三个可迁系组成: (i) $|z|<1$, (ii) $|z|=1$ 和 (iii) $|z|>1$. 如果 $|z|<1$ 为我们的新空间 S', 则空间 S' 在群 H 之下的几何称为лобачевский 几何.

§2 射影空间

设 K 为体, 特征为 0 或 p. p 为素数.

现考查所有 $n+1$ 数组 $(a_0, a_1, \cdots, a_n)$ 的集合, $a_0, a_1, \cdots, a_n \in K$, 而 $a_0, a_1, \cdots, a_n$ 不全为零, 即所有 V_{n+1} 中的非零向量之全体. 两个这种数组 $(a_0, a_1, \cdots, a_n)$ 和 $(b_0, b_1, \cdots, b_n)$ 称为左等价, 如果 K 中有一个元素 λ 存在, 使得

$$(a_0, a_1, \cdots, a_n) = \lambda(b_0, b_1, \cdots, b_n).$$

显然, $\lambda \neq 0$. 这是个等价关系. 我们把等价的 $n+1$ 数组称为点. 这样的点的集合就称为 K 上的 n 维 (左) 射影空间, 记作 $PN_n^l(K)$. 类似地, 我们可以定义 K 上的 n 维 (右) 射影空间, 记作 $PN_n^r(K)$.

设 $A = (a_{ij})$ 为元素在 K 中的 $n+1$ 行可逆矩阵. 考查方程

$$y = xA, \tag{1}$$

而 $y=(y_0,y_1,\cdots,y_n)$ 及 $x=(x_0,x_1,\cdots,x_n)$, 这就定义了空间中的一个射影变换, 将点 $(\lambda x_0,\lambda x_1,\cdots,\lambda x_n)$ 变到 $(\lambda y_0,\lambda y_1,\cdots,\lambda y_n)$. 于是对于 K 上每一个 $n+1$ 行可逆矩阵 A 都对应着一个射影交换 (1), 但反之则未必. 实际上, 两个可逆矩阵 A 和 B 表同一射影变换, 当且仅当 K 中有一个中心元素 ρ 存在, 使得

$$A=\rho B.$$

为了证明这一点, 仅需证明: 如果变换

$$y=xA$$

将射影空间中每一点都不变, 则必有 $A=\rho I$, 而 ρ 为 K 中的中心元素. 将 $(1,0,\cdots,0)$, $(0,1,0,\cdots,0),\cdots,(0,\cdots,0,1)$ 代入

$$\lambda x=xA,$$

就可推出 A 为对角矩阵. 写

$$A=[a_0,a_1,\cdots,a_n],$$

由

$$\lambda(x_0,x_1,\cdots,x_n)=(x_0,x_1,\cdots,x_n)A$$

推出

$$\lambda x_0=x_0a_0,\quad \lambda x_1=x_1a_1,\cdots,\quad \lambda x_n=x_na_n,$$

对于所有的 $(x_0,x_1,\cdots,x_n)\neq(0,0,\cdots,0)$, 而 λ 可以依赖于 $(x_0,x_1,\cdots,x_n)$. 由 $(x_0,x_1,\cdots,x_n)=(1,1,\cdots 1)$ 推出 $\lambda=a_0=a_1=\cdots=a_n$, 因之 λ 与 $(x_0,x_1,\cdots,x_n)$ 无关而且是 K 中的一个中心元素. 因 $\lambda=\rho$, 故 $A=\rho I$.

再者, 方程

$$y=xB,$$

而 B 为 A 之逆, 表与 A 相逆之射影变换, 而且如果

$$y=xA_1,\quad y=xA_2$$

为二射影变换, 则其积

$$z=yA_2=xA_1A_2$$

也为一射影变换, 因 A_1A_2 也可逆. 这就证明了

定理 1　$PN_n^l(K)$ 中之射影变换之全体组成一群, 称为 K 上 n 维射影变换群, 此群即为 $PGL_{n+1}(K)$.

更进一步, 如果假定 (1) 中矩阵属于 $SL_{n+1}(K)$, 如此得到的射影变换组成的群就是 $PSL_{n+1}(K)$.

今设 S 为一集合, 它的点可以与 $PN_n^l(K)$ 的点一一对应, 并以 π 表此对应, 则 $PN_n^l(K)$ 中任一射影变换 T 都对应着 S 中的一个变换 $\pi T\pi^{-1}$. 显然, S 的这种变换之全体组成一群, 把集合 S 看作有这样一个群作用在它上面, 我们就得到一个 n 维 (左) 射影空间, 记作 $P_n^l(K)$. S 中的元素称为点. 在对应 π 之下, S 中的每一点 P 都对应着非零 $n+1$ 数组 $(\lambda a_0, \lambda a_1, \cdots, \lambda a_n)$ 所组成的等价类, 而有 $P\pi = (\lambda a_0, \lambda a_1, \cdots, \lambda a_n)$. 这个等价类中的任意 $n+1$ 数组都称为点 P 的一组坐标. 因之, 对应 π 就确定了 S 中的一个坐标系.

考虑 $PN_n^l(K)$ 中的一个射影变换. 如果这个变换将 $PN_n^l(K)$ 中在 π 之下对应于 P 的点 $P\pi$ 变到 $P\pi'$, 则 S 中的点 P 的集合与 $PN_n^l(K)$ 中的点 $P\pi'$ 的集合之间就有了一个一一对应, 而这个对应也在 S 中定义了一组坐标. 实际上, 对于 $PN_n^l(K)$ 中的任意一个射影变换都可以定义出 S 的一组坐标来, S 的各个这样所得到的坐标就称为 S 的可许坐标系. 由射影变换成群的性质可以推知如果确定 S 和 $PN_n^l(K)$ 之间最初的那个一一对应 π 用另外一个确定 S 的可许坐标系的对应 π' 来代替的话, 也得到同样的可许坐标系的集合.

如今, 我们可以把方程

$$y = xA, \tag{1}$$

其中 $y = (y_0, y_1, \cdots, y_n), x = (x_0, x_1, \cdots, x_n)$ 而 A 为 $n+1$ 行可逆矩阵, 用两种方法来解释. 首先, 我们可以把 $(x_0, x_1, \cdots, x_n)$ 看作 $P_n^l(K)$ 中之一点 P 在某一可许坐标系中的坐标, 而 $(y_0, y_1, \cdots, y_n)$ 为这同一点 P 在另一可许坐标系之中的坐标, 即这时我们把 (1) 式看作坐标变换. 其次, 我们可以把 $(y_0, y_1, \cdots, y_n)$ 看作点 $(x_0, x_1, \cdots, x_n)$ 在射影变换之下的像, 即这时我们把 (1) 式看作 $P_n^l(K)$ 中的射影变换.

最后我们指出, 对于 $P_n^r(K)$ 也可作同样的讨论, 但我们不去重复它了.

§3　$P_n^l(K)$ 中点的线性相关性

定义 1　设 $A^0, A^1, \cdots, A^k$ 为 $P_n^l(K)$ 中的 $k+1$ 个点. 以

$$A^i = (a_0^i, a_1^i, \cdots, a_n^i) \quad (i = 0, 1, \cdots, k)$$

表它们在一可许坐标系中之坐标. 我们说它们在 $P_n^l(K)$ 中线性相关, 如果 K 中有

不全等于零的元素 $\lambda_0, \lambda_1, \cdots, \lambda_k$ 存在, 使得

$$\sum_{i=0}^{k} \lambda_i a_j^i = 0 \quad (j = 0, 1, \cdots, n).$$

否则, 我们就说它们在 $P_n^l(K)$ 中线性无关.

为了说明点 $A^0, A^1, \cdots, A^k$ 的线性相关性为点的本身的性质, 这就必须要证明它们的线性相关性与在选取的坐标系中 $A^0, A^1, \cdots, A^k$ 的坐标的选取无关, 以及与可许坐标系的选取无关. 实际上, 设 $(b_0^i, b_1^i, \cdots, b_n^i)$ 为 A^i 在已给可许坐标系中的另一组坐标, 则

$$b_j^i = \mu_i a_j^i \quad (i = 0, 1, \cdots, k; j = 0, 1, \cdots, n),$$

而 μ_i 为 K 中的一些非零元素. 于是, 由 (1) 可以推出

$$\sum_{i=0}^{k} (\lambda_i \mu_i^{-1}) b_j^i = 0 \quad (j = 0, 1, \cdots, n).$$

再者, 令

$$y = xC$$

表 $P_n^l(K)$ 中的可许坐标变换. 在新坐标系中, 设 A^i 的坐标为 $(b_0^i, b_1^i, \cdots, b_n^i)$, 则

$$(b_0^i, b_1^i, \cdots, b_n^i) = (a_0^i, a_1^i, \cdots, a_n^i)C \quad (i = 0, 1, \cdots, k).$$

于是

$$\sum_{i=0}^{k} \lambda_i (b_0^i, b_1^i, \cdots, b_n^i) = (\sum_{i=0}^{k} \lambda_i (a_0^i, a_1^i, \cdots, a_n^i))C = 0,$$

因此 $P_n^l(K)$ 中点的线性相关性为点的性质. 我们可以形式地写作

$$\sum_{i=0}^{k} \lambda_i A^i = 0$$

借助于第三章中所讨论的行向量的线性相关性, 我们可以用以下的定义来表明点 $A^0, A^1, \cdots, A^k$ 的相关性.

I. 如果 $(a_0^i, a_1^i, \cdots, a_n^i)$ $(i = 0, 1, \cdots, k)$ 为 $A^0, A^1, \cdots, A^k$ 在一已知可许坐标系中的坐标, 则 $A^0, A^1, \cdots, A^k$ 线性相关之充要条件为这 $k+1$ 个行向量

$$(a_0^i, a_1^i, \cdots, a_n^i) \quad (i = 0, 1, \cdots, k)$$

在 K 上线性相关.

II. $A^0, A^1, \cdots, A^k$ 线性无关的充要条件为矩阵

$$\begin{pmatrix} a_0^0 & a_1^0 & \cdots & a_n^0 \\ a_0^1 & a_1^1 & \cdots & a_n^1 \\ \cdots & \cdots & \cdots & \cdots \\ a_0^k & a_1^k & \cdots & a_n^k \end{pmatrix}$$

的秩为 $k+1$.

我们立刻可以得出以下的推论:

定理 1 $P_n^l(K)$ 中的任意 m 个点, 而 $m > n+1$, 必线性相关.

定义 2 如果一点 A 可写作

$$\lambda A - \sum_{i=0}^{k} \lambda_i A^i = 0$$

或

$$\lambda A = \sum_{i=0}^{k} \lambda_i A^i,$$

而 λ 为 K 中非零元素, 则 A 称为线性相关于 $A^0, A^1, \cdots, A^k$.

显然, 在一已知可许坐标系中, 以下 $n+1$ 个点

$$A^i = (\delta_{i0}, \delta_{i1}, \cdots, \delta_{in}) \quad (i = 0, 1, \cdots, n)$$

线性无关, 其中 $\delta_{ii} = 1; \delta_{ij} = 0$ 若 $i \neq j$. 而任意一点

$$A = (a_0, a_1, \cdots, a_n)$$

可以表成

$$A = \sum_{i=0}^{n} a_i A^i.$$

因之 $P_n^l(K)$ 中任意一点都线性相关于这 $n+1$ 个点. 它们称为已知坐标系的标准单纯形.

我们注意, 如果 $A^0, A^1, \cdots, A^k$ 为 $P_n^l(K)$ 中 $k+1$ 个线性相关的点, 则它们在任意可许坐标系中的坐标为 $V_{n+1}(K)$ 中 $k+1$ 个线性相关的向量; 而且反之亦然. 因此, 点的线性相关性的性质可以由向量的线性相关性的性质推出来. 我们把主要的结果写在下面:

定理 2 如果 $A^0, A^1, \cdots, A^k$ 线性无关, 如果 A 线性相关于它们, 并且

$$\lambda A = \sum_{i=0}^{k} \lambda_i A^i,$$

则 $k+1$ 数组 $(\lambda_0,\lambda_1,\cdots,\lambda_k)$ 所属的等价 $k+1$ 数组类唯一确定.

定理 3 如果 $B^0,B^1,\cdots,B^h$ 线性相关于 $A^0,A^1,\cdots,A^k$, 而 P 线性相关于 $B^0,B^1,\cdots,B^h$, 则 P 也线性相关于 $A^0,A^1,\cdots,A^k$.

定理 4(替换定理) 设 $B^0,B^1,\cdots,B^h$ 为 $h+1$ 个线性无关的点, 并假定它们都线性相关于 $A^0,A^1,\cdots,A^k$, 则 $h\leqslant k$, 而且我们可以在 $A^0,A^1,\cdots,A^k$ 中找出 $k-h$ 个点 $A^{i_{h+1}},\cdots,A^{i_k}$, 使得线性相关于 $A^0,A^1,\cdots,A^k$ 的点也线性相关于 $B^0,B^1,\cdots,B^h,A^{i_{h+1}},\cdots,A^{i_k}$.

§4 线性子空间

定义 1 $P_n^l(K)$ 中之一子集称为 $P_n^l(K)$ 中的一个线性子空间, 如果它包括所有线性相关于其中任意有限个点的点.

例如, 依定理 3.3, $P_n^l(K)$ 中线性相关于 $k+1$ 个已知点 $A^0,A^1,\cdots,A^k$ 的集合为一子空间, 此子空间记作 $L(A^0,A^1,\cdots,A^k)$.

定义 2 设 L 为 $P_n^l(K)$ 中一子空间. 如果 $L=L(A^0,A^1,\cdots,A^k)$, 则 $A^0,A^1,\cdots,A^k$ 称为 L 的生成元. 如果它们是线性无关的, 则它们就称为基.

我们现在指出在 $P_n^l(K)$ 的线性子空间的集合与 $V_{n+1}(K)$ 的不是仅由零向量所组成的向量子空间的集合之间存在着一个一一对应的关系. 如果 L 是 $P_n^l(K)$ 的子空间, 则其中的点在一可许坐标系中的坐标和 $(0,0,\cdots,0)$ 一起组成 $V_{n+1}(K)$ 中与 L 相对应的向量子空间; 如果 V 为 $V_{n+1}(K)$ 中的一个向量子空间, 则 $P_n^l(K)$ 中那些点在一可许坐标系中其坐标属于 V 者组成与 V 相应的子空间. 因此, $P_n^l(K)$ 中线性子空间的性质可以从向量子空间的相当的性质推出来, 我们只把结果写在下面而不去证明它们.

定理 1 $L(A^0,A^1,\cdots,A^k)$ 的任何线性无关子集最多包有 $k+1$ 个线性无关的点.

定理 2 $P_n^l(K)$ 的任何非空线性子空间 L 都有基.

定理 3 设 $A^0,A^1,\cdots,A^k$ 为 $P_n^l(K)$ 中一非空子空间 L 的基, 如果 $B^0,B^1,\cdots,B^k$ 为 L 中任意 $k+1$ 个线性无关的点, 则

$$L=L(A^0,A^1,\cdots,A^k)=L(B^0,B^1,\cdots,B^k).$$

更进一步, 基中点的个数都一样.

定义 3 $P_n^l(K)$ 中一非空线性子空间 L 的任何一组基中点的个数减去 1 称为 L 的维数. 空集定义为 -1 维的, 0 维线性子空间称为点, 1 维线性子空间称为线, 2 维线性子空间称为平面, $n-1$ 维线性子空间称为超平面.

我们有以下重要定理:

定理 4 $P_n^l(K)$ 的任意一个 k 维线性子空间都是一个 $P_k^l(K)$.

【证】 设 $A^0, A^1, \cdots, A^k$ 为此 k 维线性子空间的一组基, 则此子空间中任意点 Q 皆可表为

$$Q = \sum_{i=0}^{k} \lambda_i A^i,$$

而 $k+1$ 数组 $(\lambda_0, \lambda_1, \cdots, \lambda_k)$ 除开左等价外由 Q 点唯一决定. 这就建立了此子空间的点与 $PN_k^l(K)$ 的点之间的一个一一对应. 现在设 $B^0, B^1, \cdots, B^k$ 为此子空间的另一组基. 我们有

$$B^i = \sum_{j=0}^{k} b_{ij} A^j \quad (i = 0, 1, \cdots, k)$$

及

$$A^i = \sum_{j=0}^{k} a_{ij} B^j \quad (i = 0, 1, \cdots, k),$$

于是

$$A^i = \sum_{j=0}^{k} \sum_{l=0}^{k} a_{ij} b_{jl} A^l \quad (i = 0, 1, \cdots, k).$$

因为 $A^0, A^1, \cdots, A^k$ 线性无关, 所以这是一个恒等式, 因之矩阵

$$A = (a_{ij})$$

及

$$B = (b_{ij})$$

互为逆矩阵, 这就是说 A 和 B 都是可逆的.

今如果

$$Q = \sum_{i=0}^{k} \lambda_i A^i,$$

则

$$Q = \sum_{i=0}^{k} \sum_{j=0}^{k} \lambda_i a_{ij} B^j = \sum_{j=0}^{k} \mu_j B^j,$$

而

$$\mu_j = \sum_{i=0}^{k} \lambda_i a_{ij}. \tag{1}$$

于是, 由 $A^0, A^1, \cdots, A^k$ 到 $B^0, B^1, \cdots, B^k$ 的基底变换就给出 $P_k^l(K)$ 中的射影变换 (1). 反之, $P_k^l(K)$ 中任一射影变换也对应于线性子空间的一个基底变换. 于是,

$P_k^l(K)$ 的任一 k 维子空间都是一个 $P_k^l(K)$, 而且每组可许坐标系中的坐标变换都对应着子空间中的一个基底变换.

现在我们来研究 $P_n^l(K)$ 的子空间所成之集合的格的结构. 以下结果可以从对应的向量子空间的结果立即推出.

定理 5　如果 L 和 M 分别为 h 和 k 维的线性子空间, 而 $L \subseteq M$, 则 $h \leqslant k$. 更进一步, 对于 L 的任一基, 我们都可添加 M 中的 $k-h$ 个点到它上面使之成为 M 的基. 又如果 $L \subseteq M$ 而 $h=k$, 则 $L=M$.

我们定义, 二个线性子空间 L 和 M 的交 $L \cap M$ 为 L 和 M 的公共元素的集合. 由线性子空间的定义可以立即推出 $L \cap M$ 也为子空间. 包含 L 和 M 的最小线性子空间称为 L 和 M 的联, 记作 $L \cup M$.

以下关于交与联的性质极易验证其成立:

$$
\begin{aligned}
&\mathrm{L}_1 \quad L \cup L = L, \quad L \cap L = L;\\
&\mathrm{L}_2 \quad L \cup M = M \cup L, \quad L \cap M = M \cap L;\\
&\mathrm{L}_3 \quad L \cup (M \cup N) = (L \cup M) \cup N,\\
&\qquad\ L \cap (M \cap N) = (L \cap M) \cap N;\\
&\mathrm{L}_4 \quad L \cup (L \cap M) = L,\ L \cap (L \cup M) = L.
\end{aligned}
$$

其中 L, M, N 都是 $P_n^l(K)$ 的子空间.

如果我们用 $d(L)$ 来表示子空间 L 的维数, 则有

定理 6　设 L 和 M 为 $P_n^l(K)$ 的线性子空间, 则

$$d(L \cup M) + d(L \cap M) = d(L) + d(M).$$

更进一步, 我们有

定理 7　如果 L, M 和 N 是 $P_n^l(K)$ 的线性子空间, 而 $L \subseteq N$, 则

$$L \cup (M \cap N) = (L \cup M) \cap N.$$

定理 8　对于 $P_n^l(K)$ 的任一线性子空间 L, 都可以找到一个子空间 L', 使得

$$P_n^l(K) = L \cup L',$$

而

$$L \cap L' = \varnothing$$

(L' 称为 L 的补空间).

定理 9　设 L 为 $P_n^l(K)$ 的线性子空间, 则对于含于 L 的任意一串单调递增子空间

$$L_0 \subset L_1 \subset \cdots \subseteq L \quad (L_i \neq L_{i+1}),$$

都可以找到一个整数 r, 使得 $L_r = L$.

在下一节中, 我们还要回来讨论这些结果.

最后我们来研究 1 维线性子空间, 即线. 我们不难证明

P_1 任意两个不同的点都在一条而且只在一条线上.

P_2 任何一线都至少包有三个点.

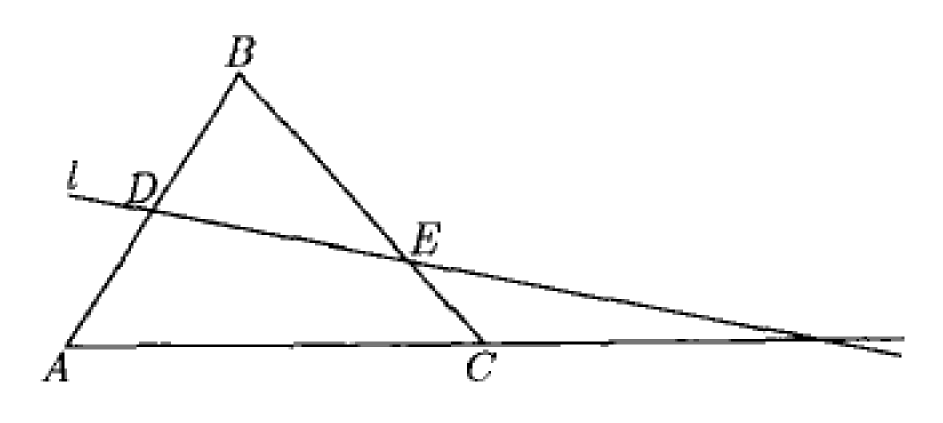
更进一步, 我们要证明

P_3 如果一条直线与一个三角形的两边相交 (不在它们的交点), 则必与第三边相交.

【证】 设三角形的顶点为 A, B, C. 设 D 和 E 分别为线 l 与 AB 和 BC 的交点, 则

$$D = aA + bB, E = cB + dC.$$

因为 l 不通过 B 点, 所以 $a \neq 0, d \neq 0$. D 和 E 所确定的直线上的点必可表成



$$xD + yE = xaA + (xb + yc)B + ydC,$$

而且对于任意不全为零的 x 和 y, 它们都是 l 上的点. 因为我们可以选取 λ 和 μ 使得

$$\lambda b + \mu c = 0,$$

而 λa 和 μd 不全为零, 所以 P_3 就证明了.

以下我们将给出线性子空间的另一定义, 并把它称之为束. 这个定义依赖于线的概念.

定义 4 $P_n^l(K)$ 中的一个点集称为一个束, 如果它包有通过它里面任意两点的线上的点的全体.

设 $A^0, A^1, \cdots, A^k$ 为 $P_n^l(K)$ 中 $k+1$ 个点. 我们先求通过 A_0 和 A_1 两点的线上的点的集合, 然后, 我们再求通过上面这个集合中的一点和 A_2 的线上的点的集合, 这样继续下去一直进行到 A^k, 最后得到的点集显然是一束, 称之为由 $A^0, A^1, \cdots, A^k$ 所定义的束. 显然, 将 $A^0, A^1, \cdots, A^k$ 重新排一下, 用上面这种方法, 仍然得出同一个束来.

我们更有以下的性质:

P_4 存在有由 $n+1$ 个点所成之有限集合, 它们所确定的束为整个空间, 而由任意少于 $n+1$ 个点所确定的束却不能是整个空间.

实际上,

$$(1,0,\cdots,0),\quad (0,1,0,\cdots,0),\cdots,\quad (0,\cdots,0,1)$$

就是适合我们要求的 $n+1$ 个点. 而任意 $m+1(<n+1)$ 个点顶多确定一个 m 维子空间.

§5　关于射影几何的公理化处理

上节中的性质 P_1,P_2,P_3 和 P_4 有时被用作射影几何的公理, 更确切地说, 我们有下面的定义:

设 $n>1$, n 维射影空间为一适合 P_1,P_2,P_3 和 P_4 的点和线的集合.

在上节中, 我们证明了由射影空间原来的定义可以推出这个定义来; 当 $n>2$ 时, 由这个定义也可推出原来的定义. 这件事实的证明只不过是在射影空间中引进坐标, 这可以在任何射影几何的古典教本中找到 (例如 O.Veblen and J.W.Young, Projective Geometry).

当 $n=2$ 时,P_1,P_2,P_3 和 P_4 不足以刻画出以前所讨论的 2 维射影空间来, 更确切地说, 对于 §2 所定义的 $n(>1)$ 维射影空间和本节中所定义的 $n(>2)$ 维射影空间, 我们能够证明以下著名的 Desargue 定理.

Desargue **定理**　设 ABC 和 $A'B'C$ 为两个三角形. 如果 AA',BB',CC' 通过一点, 则 AB 和 $A'B'$ 的交点, BC 和 $B'C'$ 的交点以及 AC 和 $A'C'$ 的交点共线; 而且反之亦然.

在 $n=2$ 时, 我们不能从 P_1,P_2,P_3 和 P_4 推出这条定理来.

在引进坐标的过程中, 这条定理是很基本的, 如果本节中所定义的 2 维射影空间亦适合 Desargue 定理, 则可以在它里面引进坐标因而是 §2 中所定义的射影空间. Desargue 定理在其中不成立的 2 维射影空间称为非 Desargue 空间. (关于非 Desargue 空间, 读者可以参看以下论文: O.Veblem and J. H. M. Wedderburn, Trans. Amer. Math. Soc., 84(1907), 379~388; M. Hall, Projective Planes, Trans. Amer. Math. Soc., 54(1943), 229~277; 以及 Ruth. Monfang 发表于 Math. Annalen, 105~110 卷上的六篇论文.)

射影几何的另一组公理是格论方面的. 首先我们举出以下公理:

L_1　　$L\cup L=L,\qquad L\cap L=L;$

L_2　　$L\cup M=M\cup L,\quad L\cap M=M\cap L;$

L_3　　$L\cup(M\cup N)=(L\cup M)\cup N,\quad L\cap(M\cap N)=(L\cap M)\cap N;$

L_4　　$L\cup(L\cap M)=L,\quad L\cap(L\cup M)=L.$

如果 $L\cup M=M$ 或同样地 $L\cap M=L$, 就定义为 $L\subseteq M$.

L$_5$ 如果$L \subseteq N$, 则 $L \cup (M \cap N) = (L \cup M) \cap N$;

L$_6$ 对于每个 L 都有一个 L' 使得对于所有 M 都有

$$M \subseteq L \cup L' \text{及} L \cap L' \subseteq M.$$

L$_7$ 对于每个 L, 如果有含于 L 的单调递增链:

$$L_0 \subset L_1 \subset L_2 \subset \cdots \subseteq L \quad (L_i \neq L_{i+1}),$$

则必有一整数 r 存在, 使得 $L_r = L$.

适合 L$_1$, L$_2$, L$_3$ 和 L$_4$ 的一组元素集合称为一格, 条件 L$_5$, L$_6$ 及 L$_7$ 分别称为模性, 补性及链条件. 我们在上节中已经证明, n 维射影空间所有的子空间的集合为一有模性, 补性及链条件的格. 反之, 我们可以证明, 任一有模性, 补性及链条件的格必为射影空间的直接和. 关于这个定理的证明读者可以看 G. Birkhoff, Annals of Math., 36 (1935), 433~454 及 Menger, Annals of Math., 37(1936), 456~482 的论文.

最后我们指出, 如果用 P$_1$, P$_2$, P$_3$ 和 P$_4$ 来刻画射影空间, 我们只需要两种对像, 即点和线; 而如果用 L$_1$ ~ L$_7$ 来刻画射影空间, 我们需要全体子空间. 因之, 第一种方法的好处是可以用低维子空间来刻画几何, 而第二种方法的好处则在于有对称性, 即对偶性.

§6 线性子空间的方程及对偶原理

在讨论线性子空间的方程以前, 我们先引进子空间的矩阵表示法.

设 S_k 为 $P_n^l(K)$ 中的一个 k 维线性子空间, 并设 $A^0, A^1, \cdots, A^k$ 为 S_k 的一组基, 在一可许坐标系中, 令 $a^0 = (a_0^0, a_1^0, \cdots, a_n^0), a^1 = (a_0^1, a_1^1, \cdots, a_n^1), \cdots, a^k = (a_0^k, a_1^k, \cdots, a_n^k)$ 表点 $A^0, A^1, \cdots, A^k$ 的坐标. 我们造出矩阵

$$L = \begin{pmatrix} a^0 \\ a^1 \\ \vdots \\ a^k \end{pmatrix},$$

这是个 $(k+1, n+1)$ 型的矩阵, 而它的秩为 $k+1$. 我们把它称之为在已知可许坐标系中 S_k 的一个矩阵表示. 显然, 在 $P_n^l(K)$ 中用一个 $n+1$ 行可逆矩阵 T 来变换坐标, 则 S_k 在新的坐标系中的矩阵表示就是 LT. 型为 $(k+1, n+1)$ 的两个矩阵 L 和 M 在同一可许坐标系中表同一子空间 S_k 当且仅当有一 $k+1$ 行可逆矩阵 Q 存在, 使得

$$L = QM.$$

再者, 如一 h 维子空间 S_h 含于一 k 维子空间 S_k 中, 并设 L 和 M 分别为它们在同一可许坐标系中的矩阵表示, 则有一 $(h+1,k+1)$ 型而 $h+1$ 秩的矩阵 Q 存在, 使得

$$L = QM.$$

而且, 反之亦然.

同样, $P_n^r(K)$ 中一 k 维线性子空间 Σ_k 可以用一个矩阵

$$(b^0, b^1, \cdots, b^k)$$

表出, 如果 $b^0 = (b_0^0, b_1^0, \cdots, b_n^0)', b^1 = (b_0^1, b_1^1, \cdots, b_n^1)', \cdots, b^k = (b_0^k, b_1^k, \cdots, b_n^k)'$ 是 Σ_k 的基中的点在一可许坐标系中之坐标. 显然, 这个矩阵是 $(n+1,k+1)$ 型而 $k+1$ 秩的.

今研究一左射影空间 $P_n^l(K)$ 和一右射影空间 $P_n^r(K)$. 在这每一个空间中我们都确定任意选的可许坐标系, 并且我们说它们相联. 我们先来说明如何将 $P_n^l(K)$ 中的一个可许坐标系与 $P_n^r(K)$ 中的一个相联.

假定 $P_n^l(K)$ 中给了一组新的坐标系, 设从原先选取的坐标系到这组新的坐标系的变换为

$$y = xA,$$

然后我们就把 $P_n^l(K)$ 中这组新的坐标系与由变换

$$y' = A^{-1}x'$$

从 $P_n^r(K)$ 中原先选定的坐标系所得的坐标系相联. 显然, 可以证明两个空间的可许坐标系间的相联对应是 1 对 1 的, 而且当任意一对相联坐标系确定后, 这个对应被依上述规则所唯一确定.

今考虑 $P_n^l(K)$ 中的一个 k 维线性子空间 S_k, 并且让 L 为 S_k 在一可许坐标系中的矩阵表示, 考虑方程组

$$Lx' = 0, \tag{1}$$

而 $x = (x_0, x_1, \cdots, x_n)$. 因为 L 为 k 维子空间的矩阵表示, 所以 L 是 $(k+1,n+1)$ 型而 $k+1$ 秩的矩阵; 因之齐次方程组 (1) 的解组成右空间中的一个 $n-k$ 维的向量子空间. 将此向量子空间中的非零向量取作 $P_n^r(K)$ 中相联坐标系中一线性子空间的点的坐标, 则其维数为 $n-k-1$, 将它记作 Σ_{n-k-1}, 以 U 表 Σ_{n-k-1} 在相联坐标系中的一个矩阵表示, 则

$$LU = 0. \tag{2}$$

可是, 因为 U 是一个 $n-k-1$ 维子空间的矩阵表示, 适合方程组

$$xU=0$$

的向量组成左空间中的一个 $k+1$ 维的向量子空间. 这个子空间的非零向量可以看作 $P_n^l(K)$ 中一个 k 维子空间的坐标. 据 (2), 这个子空间包有 S_k 的所有点, 因之与 S_k 相重合. 于是 S_k 决定了 Σ_{n-k-1}; 而反过来, Σ_{n-k-1} 又决定了 S_k, 我们就说它们相联.

我们来证明这个相联关系与特别选的 $P_n^l(K)$ 与 $P_n^r(K)$ 中相联的坐标系无关. 设

$$y=xA$$

为 $P_n^l(K)$ 中之坐标变换, 而

$$y'=A^{-1}x'$$

为 $P_n^r(K)$ 中相联的坐标变换, 即 S_k 与 Σ_{n-k-1} 在这组新的相联的坐标系中的矩阵表示分别为 LA 和 $A^{-1}U$, 我们仍然有

$$(LA)(A^{-1}U)=L(AA^{-1})U=LU=0,$$

因之得证. 子空间 S_k 和 Σ_{n-k-1} 称为对偶线性子空间. 因之, 我们证明了

定理 1 对于 $P_n^l(K)$ 的每一个线性子空间 S_k 都有 $P_n^r(K)$ 中的一个对偶线性子空间 Σ_{n-k-1} 与之对应, 而且, 反之亦然.

如果我们取 $P_n^r(K)$ 中一 $n-k-1$ 维的线性子空间 Σ_{n-k-1} 在一可许坐标系中的矩阵表示为 U, 则 S_k 就是 $P_n^l(K)$ 中在相联坐标系中适合方程

$$xU=0 \tag{3}$$

的所有的点. 因而我们把 (3) 称为线性子空间 S_k 的方程.

其次我们证明

定理 2 两个线性子空间的交的对偶为它们对偶的联, 而且, 反之亦然.

【证】 设 S_p 和 S_q 为 $P_n^l(K)$ 中的两个线性子空间. 设它们的方程分别为

$$xU=0 \quad 和 \quad xV=0,$$

则 S_p 和 S_q 的交就是由这方程组所定义的. 假定矩阵 $(U\ V)$ 的秩为 $n-k$, 则 S_p 和 S_q 的交是一个 k 维子空间 S_k. 写

$$U=(u_j^i)\quad \begin{pmatrix} i=0,1,\cdots,n-p-1 \\ j=0,1,\cdots,n \end{pmatrix},$$

$$V = (v_j^i) \quad \begin{pmatrix} i = 0, 1, \cdots, n-q-1 \\ j = 0, 1, \cdots, n \end{pmatrix},$$

则下面这 $2n-p-q$ 个点:

$$(4) \qquad \begin{pmatrix} u_0^i \\ u_1^i \\ \vdots \\ u_n^i \end{pmatrix} (i = 0, 1, \cdots, n-p-1), \qquad \begin{pmatrix} v_0^i \\ v_1^i \\ \vdots \\ v_n^i \end{pmatrix} (i = 0, 1, \cdots, n-q-1)$$

就线性相关于其中的 $n-k$ 个线性无关的点. 因之 S_p 和 S_q 的对偶 Σ_{n-p-1} 和 Σ_{n-q-1} 就属于一个 Σ_{n-k-1}, 而它是 S_k 的对偶. 再者, 因为任意含 Σ_{n-p-1} 和 Σ_{n-q-1} 的线性子空间必然包含 (4) 中的 $2n-p-q$ 个点, 而其中有 $n-k$ 个线性无关, 所以没有更小的子空间既包有 Σ_{n-p-1} 又包有 Σ_{n-q-1}. 因之, Σ_{n-k-1} 就是 Σ_{n-p-1} 与 Σ_{n-q-1} 的联.

于是, 立即得到下面的推论:

系理 如果 $S_p \subseteq S_q$, 则 $\Sigma_{n-p-1} \supseteq \Sigma_{n-q-1}$.

我们已经在 $P_n^l(K)$ 与 $P_n^r(K)$ 的子空间之间建立了一个对应关系, 而交与联分别对应于联与交. 如果我们对于 $P_n^l(K)$ 证明了一条定理, 而这个证明只依赖于线性子空间的性质及它们交与联的性质, 则这个对应就使我们马上写出 $P_n^r(K)$ 的一条定理而不必再去证明它. $P_n^l(K)$ 和 $P_n^r(K)$ 的定理间的关联称为射影空间的对偶原理.

对于每个体 K, 我们可以造一个体 $\bar{K}$ 与 K 反同构: 对于 K 中每个元素 a, 我们让一个符号 $\bar{a}$ 与之相关. 如果我们定义

$$\bar{a} + \bar{b} = \overline{a+b}, \quad \bar{a} \cdot \bar{b} = \overline{b \cdot a},$$

则这些符号的全体显然组成一体 $\bar{K}$ 与 K 反同构. 现考查右射影空间 $P_n^r(K)$ 与左射影空间 $P_n^l(\bar{K})$. 我们可以在 $P_n^r(K)$ 和 $P_n^l(\bar{K})$ 的点之间建立一个一一对应的关系和它们的可许坐标系之间建立一个一一对应关系. 在 $P_n^r(K)$ 和 $P_n^l(\bar{K})$ 中选定了相应的可许坐标系之后, 点

$$(a_0^i, a_1^i, \cdots, a_n^i)' \quad 和 \quad (\overline{a_0^i}, \overline{a_1^i}, \cdots, \overline{a_n^i})$$

就一一对应. 而 $P_n^r(K)$ 中从原坐标系经变换 T 得到的一个坐标系就与 $P_n^l(\bar{K})$ 中从原坐标系经变换 $\bar{T}'$ 得到的一个坐标系相对应. 在此对应之下, 线性相关性是保持的. 更进一步, k 维线性子空间对应于 k 维线性子空间, 交对应于交, 而联对应于联. 因之, 依对偶原则如果我们在 $P_n^l(K)$ 中有一条定理, 而这条定理只与线性子空间

$S_p, S_q, \cdots$ 以及它们的交与联有关, 我们就得到 $P_n^l(\bar{K})$ 中的一条定理, 而这条定理只与子空间 $S_{n-p-1}, S_{n-q-1}, \cdots$ 以及它们的联与交有关. 如果 K 为域, 则 $K=\bar{K}$, 因之, 对偶原理在 $P_n^l(K)$ 中成立. 最后, 如果原定理对于所有基础体 K 都成立, 则对于 $P_n^l(\bar{K})$ 亦成立, 因之, 对偶原理对于 $P_n^l(K)$ 亦成立.

§7 标准单纯形

定义 1 $k+1$ 个有序的线性无关的点称为一个 k-单纯形.

定理 1 在射影群之下, k-单纯形的全体组成一个可迁集.

本定理可由下列事实推出: 总有一个射影变换将任一 k-单纯形变到由下列 $k+1$ 个线性无关的点:

$$(\delta_{i0}, \delta_{i1}, \cdots, \delta_{in}) \quad (0 \leqslant i \leqslant k)$$

所组成的 k-单纯形.

定义 2 n-单纯形称为标准单纯形.

定理 2 将一个 n-单纯形不变的射影变换所组成的群与以对角矩阵为其矩阵的射影变换所组成的群同构.

【证】 依定理 1, 只要证明定理对于由 $n+1$ 个点

$$A^i = (\delta_{i0}, \delta_{i1}, \cdots, \delta_{in}) \quad (0 \leqslant i \leqslant n)$$

所组成的 n-单纯形成立即可. 由

$$A^i = \rho_i A^i T \quad (0 \leqslant i \leqslant n)$$

可以推出 T 为对角矩阵.

定义 3 $n+2$ 个有序点称为组成一标架, 如果其中任意 $n+1$ 个都线性无关.

定理 3 标架的全体组成一可迁集.

【证】 依定理 1, 我们可以取标架的前 $n+1$ 个点为

$$A^i = (\delta_{i0}, \delta_{i1}, \cdots, \delta_{in}) \quad (0 \leqslant i \leqslant n).$$

令

$$A^{n+1} = (a_0, a_1, \cdots, a_n)$$

为标架的第 $n+2$ 个点. 因为它不与 $A^1, A^2, \cdots, A^n$ 线性相关, 所以 $a_0 \neq 0$, 同理

$a_i \neq 0$ 对 $0 \leqslant i \leqslant n$. 因之, 变换

$$(y_0, y_1, \cdots, y_n) = (x_0, x_1, \cdots, x_n) \begin{pmatrix} a_0^{-1} & & & 0 \\ & a_1^{-1} & & \\ & & \ddots & \\ 0 & & & a_n^{-1} \end{pmatrix}$$

将 $A^0, A^1, \cdots, A^n$ 不变而将 A^{n+1} 变到 $(1, 1, \cdots, 1)$. 因之, 每个标架都可以变到

$$(\delta_{i0}, \delta_{i1}, \cdots, \delta_{in}) \ (0 \leqslant i \leqslant n) \quad 和 \quad (1, 1, \cdots, 1).$$

定理证毕.

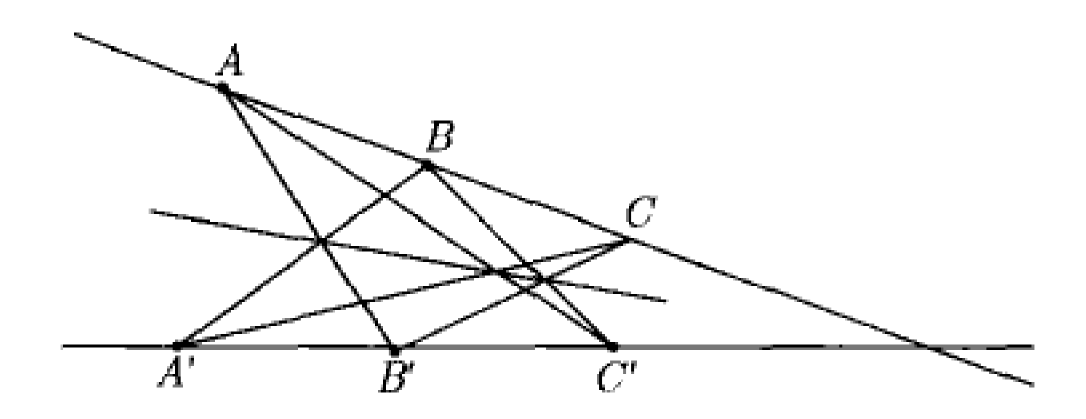
定理 4　将一个固定标架不变的射影变换的全体所组成的群与以纯量矩阵为矩阵的射影变换之全体所组成的群同构.

【证】　依定理 2, 只要证明: 如果一对角矩阵不变 $(1, 1, \cdots, 1)$, 则必是纯量矩阵. 这一点是显然的.

以下关于基础体 K 交换性的判别标准是定理 4 的直接推论.

定理 5　基础体是域当且仅当将一标架不变的射影变换只是单位变换.

【备注】　通常 Pappus 定理用来判定基础体的交换性, 我们把它叙述如下:



Pappus**定理**　如果 A, B, C 和 A', B', C' 是两条在同一平面上的直线上的三点形, 则 AB' 和 $A'B$ 的交点, AC' 和 $A'C$ 的交点以及 BC' 和 $B'C$ 的交点共线.

§8　仿射空间

我们以上所用的 $P_n^l(K)$ 中的点的坐标 $(x_0, x_1, \cdots, x_n)$ 称为齐次坐标. 如果 $x_0 \neq 0$, 我们可以用 $(1, \xi_1, \cdots, \xi_n)$ 而 $\xi_i = x_0^{-1} x_i (1 \leqslant i \leqslant n)$, 来表这一点. $(\xi_1, \cdots, \xi_n)$ 就称之为这一点的非齐次坐标. 注意, 只有齐次坐标中 $x_0 \neq 0$ 的点才有非齐次坐标; 这些点称之为有穷点, $x_0 = 0$ 的点称为无穷远点. 无穷远点之全体组成一个 $n-1$ 维子空间, 称为无穷远超平面. 无穷远超平面的方程是 $x_0 = 0$.

射影变换

$$x_i = \lambda \sum_{j=0}^{n} y_j a_{ji} \quad (i = 0, 1, \cdots, n) \tag{1}$$

可写成非齐次形

$$\xi_i = (a_{00} + \sum_{j=1}^{n} \eta_j a_{j0})^{-1}(a_{0i} + \sum_{j=1}^{n} \eta_j a_{ji}),$$

而 $\eta_j = y_0^{-1} y_j (j = 1, 2, \cdots, n)$.

将无穷远超平面取作绝对, 我们就得到 n 维仿射几何学. 确切地说, n 维仿射空间由 n 维射影空间中所有有穷点组成, 即由所有 n 数组 $(\xi_1, \cdots, \xi_n)$ 组成. 而 n 维仿射空间的变换群由将绝对 $x_i = 0$ 不变的所有射影变换组成. 如果变换 (1) 将 $x_0 = 0$ 不变, 我们有

$$a_{i0} = 0 \quad 对一切 i \neq 0.$$

取非齐次坐标就有

(2) $$\xi_i = a_{00}^{-1} \left(a_{0i} + \sum_{j=1}^{n} \eta_j a_{ji} \right).$$

写成矩阵形状就有

$$(\xi_1, \cdots, \xi_n) = a(\eta_1, \cdots, \eta_n)A + (\alpha_1, \cdots, \alpha_n),$$

其中 $a \neq 0, A = A^{(n)}$ 可逆. 写成向量形状就有

(3) $$\xi = a\eta A + \alpha,$$

其中 $\xi = (\xi_1, \cdots, \xi_n), \eta = (\eta_1, \cdots, \eta_n)$, 而 $\alpha = (\alpha_1, \cdots, \alpha_n)$. 变换 (3) 的全体组成一群, 称为 n 维仿射群. 仿射几何就是研究仿射空间在仿射群之下不变的性质的.

现在我们来研究仿射群, 将它表之为 Σ. 变换

$$\xi = \eta + \alpha$$

称为平移. 显然, 平移之全体组成 Σ 之一 Abel 子群 Γ, 而 Γ 为 Σ 之正规子群. 商群 Σ/Γ 与等价群

(4) $$\xi = a\eta A$$

同构, 因之与 K^* 和 $PGL_n(K)$ 的直积同构.

仿射空间是可迁的, 其稳定群恰是等价群.

我们把 n 维仿射空间对于它的 k 维 $(0 \leqslant k \leqslant n)$ 向量子空间的陪集称为 k 维仿射子空间. 特别, 0 维仿射子空间是点, 1 维仿射子空间是线, 2 维仿射子空间是面, $n-1$ 维仿射子空间称为超平面.

在非齐次坐标系中, 仿射空间中超平面的方程为

$$\xi_1 a_1 + \cdots + \xi_n a_n = b.$$

仿射空间中两张超平面并不永远相交. 一般地, 两个线性子空间如不相交就称为平行. 显然, 仿射变换将平行的线性子空间变到平行的线性子空间.

§9 仿射几何的基本定理

本节之目的为证明仿射几何的基本定理.

定理 1 设 $n>1$, 体 K 上 n 维仿射空间中任意一个将线变到线 (同时, 当 $n\geqslant 3$ 而 $K=F_2$ 时还要求将面变到面) 的一一变换必具形状

$$(1) \qquad (x_1,\cdots,x_n)\to(x_1,\cdots,x_n)^\sigma T+(\alpha_1,\cdots,\alpha_n),$$

其中 $T=T^{(n)}$ 为可逆矩阵, σ 为体 K 的自同构. 反之, (1) 形的变换必是一一的, 而且将线变到线.

【证】 定理中的第二个断言显然成立. 现在来证明第一个断言. 我们对 n 施行归纳法.

(i) $n=2$. 设一对点 $(a_1,a_2),(b_1,b_2)$ 分别变到了 $(c_1,c_2),(d_1,d_2)$. 则联结 $(a_1,a_2),(b_1,b_2)$ 的线

$$(1-x)(a_1,a_2)+x(b_1,b_2)$$

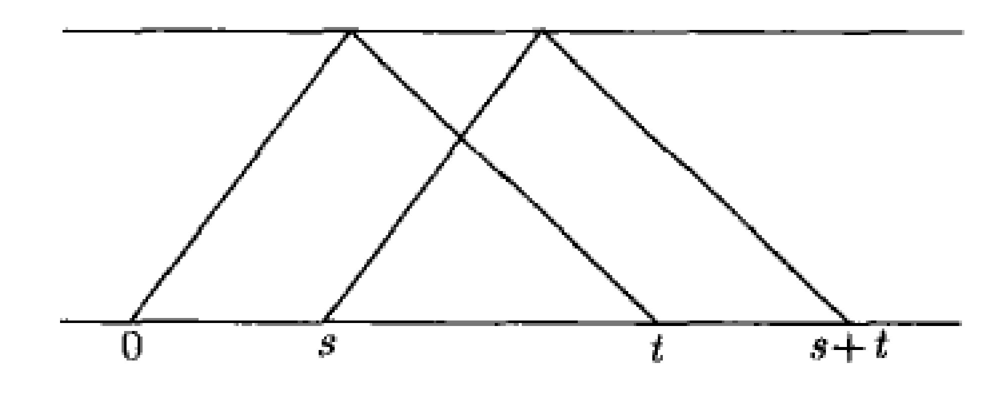
就变到联结 $(c_1,c_2),(d_1,d_2)$ 的线

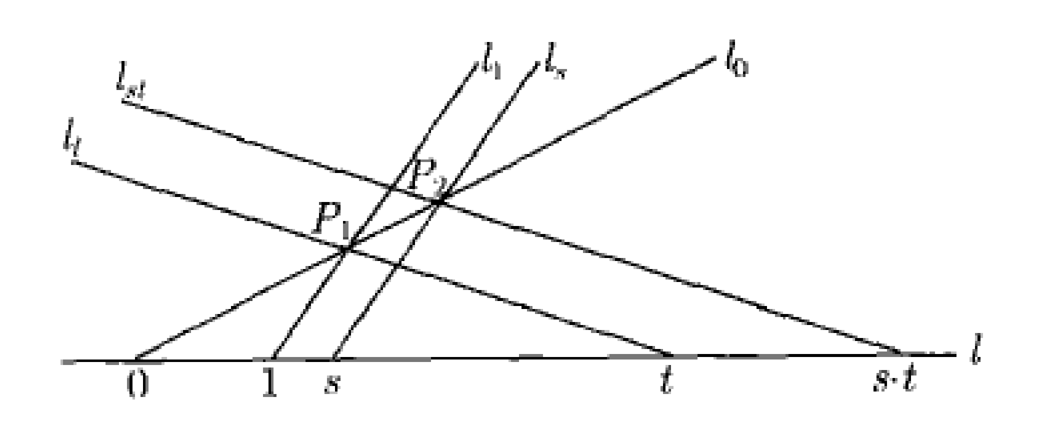
$$(2) \qquad (1-x^\sigma)(c_1,c_2)+x^\sigma(d_1,d_2).$$

我们要证明 σ 为体之自同构. 显然, 有一个形状 (1) 的仿射映射将任意一对点分别变到 (0,0) 和 (1,0), 所以只要证明我们的断言对于 $(a_1,a_2)=(c_1,c_2)=(0,0),(b_1,b_2)=(d_1,d_2)=(1,0)$ 成立就行了. 于是, 线 $(x,0)$ 就变到了线 $(x^\sigma,0)$, 而有 $1^\sigma=1,0^\sigma=0$. 那么

$$(s+t)^\sigma=s^\sigma+t^\sigma,(st)^\sigma=s^\sigma t^\sigma.$$

这可以从交与联的方法推出, 这个方法如附图所示.





第一个式子不难证明, 我们把第二个式子的证明写出来.

设 l 为由 (0, 0), (1, 0) 所决定的线. 我们用 s 来表点 $(s,0)$. 过 0 画一条线

$$l_0: \quad (xl_0, x)\ (x \in K),$$

令这条线与 l 不同. 过 1 画一条线

$$l_1: \quad (xl_1+1, x)\ (x \in K).$$

令这条线与 l 不同且与 l_0 不平行. l_0 与 l_1 的交点为

$$P_1: \quad [(l_0-l_1)^{-1}l_0, (l_0-l_1)^{-1}].$$

过 s 平行于 l_1 画一条线

$$l_s: \quad (xl_1+s, x)\ (x \in K),$$

l_s 与 l_0 的交点为

$$P_2: \quad [s(l_0-l_1)^{-1}l_0, s(l_0-l_1)^{-1}].$$

联结 P_1 与 t 的线为

$$l_t: \quad (1-y)[(l_0-l_1)^{-1}l_0, (l_0-l_1)^{-1}]+y(t,0).$$

过 P_2 平行于 l_t 画一条线

$$\begin{aligned} l_{st}: \quad & [s(l_0-l_1)^{-1}l_0, s(l_0-l_1)^{-1}] \\ & +x[t-(l_0-l_1)^{-1}l_0, -(l_0-l_1)^{-1}]. \end{aligned}$$

l_{st} 与 l 的交点为 $(st,0)$. 如果我们用 s^σ 和 t^σ 来代替 s 和 t, 那么 st 就被 $s^\sigma t^\sigma$ 所代替, 因之 $(st)^\sigma = s^\sigma t^\sigma$. 断言证毕.

现在让 $\mathscr{A}$ 表空间中的一个 1-1 变换, 且将线变到线. 显然, 任意三个不在一线上的点可用形状 (1) 的变换变到 (0, 0),(1, 0) 和 (0, 1). 故我们可以假定

$$\mathscr{A}(0,0)=(0,0), \quad \mathscr{A}(1,0)=(1,0), \quad \mathscr{A}(0,1)=(0,1).$$

由以上结果, 行使了 K 的一个自同构之后, 可以假定

$$\mathscr{A}(x,0)=(x,0)\quad (x\in K),$$
$$\mathscr{A}(0,y)=(0,y^{\sigma})\quad (y\in K),$$

其中 σ 为 K 之自同构. 因之, 通过 $(x,0)$ 且与 y 轴平行的线与通过 $(0,y)$ 且与 x 轴平行的线的交点 (x,y) 就变到 (x,y^{σ}), 即

$$\mathscr{A}(x,y)=(x,y^{\sigma}). \tag{3}$$

依 (2), 置 $(a_1,a_2)=(c_1,c_2)=(0,0),(b_1,b_2)=(x,y)$和$(d_1,d_2)=(x,y^{\sigma})$ 就有

$$\mathscr{A}(t(x,y))=(t^{\tau}(x,y^{\sigma})). \tag{4}$$

另一方面, 用 tx 和 ty 代 (3) 中的 x 和 y 就有

$$\mathscr{A}(tx,ty)=(tx,(ty)^{\sigma}). \tag{5}$$

比较 (4),(5) 就有

$$\tau=\sigma=1.$$

因之

$$\mathscr{A}(x,y)=(x,y)\quad (x,y\in K).$$

定理在 $n=2$ 的情形就被证明了.

(ii) $n>2$. 先证次之引理.

引理 满足定理 1 中条件的一一映射必将 r 维仿射子空间映到 r 维仿射子空间, 对任意 $0\leqslant r<n$.

【证】 我们用数学归纳法来证明本引理. 设 $\mathscr{A}$ 是具有定理 1 中条件的一个映射. 假定 $\mathscr{A}$ 将任何一个 $k-1(k\geqslant 2)$ 维仿射子空间映到 $k-1$ 维仿射子空间, 我们证明 $\mathscr{A}$ 也将 k 维仿射子空间映到 k 维仿射子空间.

设 $S=W+a$ 是一个 k 维仿射子空间, 这里 W 是一个 k 维向量子空间, a 是一个 n 维向量. 任取 W 的一组基 $u_1,\cdots,u_k$, 于是 $W=[u_1,\cdots,u_k]$, 这里 $[u_1,\cdots,u_k]$ 表示 W 是由 $u_1,\cdots,u_k$ 生成的子空间. 设 S 在 $\mathscr{A}$ 之下的像集为 $S'=\mathscr{A}(S)$. 设 $\mathscr{A}(a)=a'$ $(a'\in S')$. 令

$$W'=\{u'\mid u'+a'\in S'\},$$

于是有 $S'=W'+a'$. 我们只需证明 W' 是一个 k 维向量子空间.

设 $W_{k-1}=[u_1,\cdots,u_{k-1}],L=[u_k]$. 那么 $W_{k-1}+a$ 是 S 中的一个 $k-1$ 维仿射子空间, $L+a$ 是 S 中的一个 1 维仿射子空间. 根据定理的假设条件及归纳假设,

$$\mathscr{A}(W_{k-1}+a)=W'_{k-1}+a'$$

与

$$\mathscr{A}(L+a)=L'+a'$$

分别为包于 S' 中的 $k-1$ 维与 1 维的仿射子空间，且

$$W'_{k-1}\subseteq W',\quad L'\subseteq W'.$$

我们证明 $W'=W'_{k-1}+L'$ 且 $W'_{k-1}\cap L'=\{0\}$. 后一论断的正确性是显然的，因此，只需证明前一论断成立即可.

设 $u'\in W'_{k-1}, v'\in L'$ 是任意两个向量. 令 $w'=u'+v'$. 分两种情形讨论：

1° 当 $K\neq F_2$ 时，可取 $r\neq 1,0$. 令 $u''=ru'\in W'_{k-1}$，则过点 $u''+a'$ 与 $w'+a'$ 的直线

$$l_1:\quad xu''+(1-x)w'+a'\quad (x\text{跑过}K)$$

与过 a' 与 $v'+a'$ 的直线

$$l_2:\quad yv'+a'\quad (y\text{跑过}K)$$

必有交点 $u''+a'=r(r-1)^{-1}v'+a'$，因而 $w'+a'$ 位于过 $u''+a'$ 与 $v''+a'$ 的直线上: $w'+a'=r^{-1}(u''+a')+(1-r^{-1})(u''+a')$. 因为 $u''\in W'_{k-1}, v''\in L'$，故存在 $u\in W_{k-1}, v\in L$，使得

$$\mathscr{A}(u+a)=u''+a',\quad \mathscr{A}(v+a)=v''+a'.$$

那么根据定理中的条件，$\mathscr{A}$ 必将过 S 中两点 $u+a$ 与 $v+a$ 的直线映到 S' 中过两点 $u''+a'$ 与 $v''+a'$ 的直线，因而 $w'+a'\in S', w'\in W'$.

2° 当 $K=F_2$ 时. 这时，$\mathscr{A}$ 不仅将线映到线，还将面映到面. 设 $\mathscr{A}(u+a)=u'+a', \mathscr{A}(v+a)=v'+a', u\in W_{k-1}, v\in L$. 那么 $\mathscr{A}$ 必将面 $[u,v]+a$ 映到 S' 中的面，这个面自然就是 $[u',v']+a'$，因而 S' 包有这个面上的一点 $w'+a'$，故 $w'\in W'$.

由 1° 及 2° 知，$W'_{k-1}+L'\subseteq W'$. 类似的讨论可以推得 $W'\subseteq W'_{k-1}+L'$. 因而 $W'=W'_{k-1}+L'$ 是一个 k 维子空间. 于是引理得证.

现在我们用数学归纳法来完成定理 1 的证明. 假设对于 $n-1$ $(n\geqslant 3)$ 维仿射空间来说，定理 1 成立，今证明对于 n 维仿射空间来说，定理 1 也成立.

设 $\mathscr{A}$ 是具有定理 1 中条件的一个映射，那么，施行一个形如 (1) 的映射之后，则可使原点不动. 因此，不失一般性，可设 $\mathscr{A}(0)=0$. 设

$$\begin{aligned}
&\mathscr{A}(1,0,0,\cdots,0)=(a_{11},a_{12},a_{13},\cdots,a_{1n}),\\
&\mathscr{A}(0,1,0,\cdots,0)=(a_{21},a_{22},a_{23},\cdots,a_{2n}),\\
&\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\\
&\mathscr{A}(0,0,\cdots,0,1)=(a_{n1},a_{n2},a_{n3},\cdots,a_{nn}).
\end{aligned}$$

由引理可知, $\mathscr{A}$ 必将线性无关的向量组映到线性无关向量组. 因之, 向量组 $(a_{11}, a_{12}, \cdots, a_{1n}), (a_{21}, a_{22}, \cdots, a_{2n}), \cdots, (a_{n1}, a_{n2}, \cdots, a_{nn})$ 线性无关. 令

$$T = \begin{pmatrix} a_{11} & \cdots & a_{1n} \\ \vdots & \cdots & \vdots \\ a_{n1} & \cdots & a_{nn} \end{pmatrix},$$

则施行一个形如 (1) 的映射

$$(x_1, \cdots, x_n) \to (x_1, \cdots, x_n)T^{-1}$$

之后, 必将点 $e_i = (0, \cdots, 0, \overset{(i)}{1}, 0, \cdots, 0)$ 不动 $(i = 1, 2, \cdots, n)$, 且仍保持原点不动. 令

$$A_{n-1} = \{(x_1, \cdots, x_{n-1}, 0) \mid x_i \in K\},$$

则 A_{n-1} 是一个 $n-1$ 维仿射空间. 由前面讨论, 有 $\mathscr{A}(A_{n-1}) = A_{n-1}$, 因而 $\mathscr{A}$ 在 A_{n-1} 中导出一个映射 $\mathscr{A}'$, 这个映射 $\mathscr{A}'$ 仍有定理 1 中的条件. 那么, 根据归纳假设, $\mathscr{A}'$ 必为如下形状:

$$(x_1, \cdots, x_{n-1}, 0) \to (x_1, \cdots, x_{n-1}, 0)^{\sigma} \begin{pmatrix} T_1 & 0 \\ 0 & 1 \end{pmatrix},$$

其中 T_1 为 $(n-1) \times (n-1)$ 可逆矩阵, σ 为 K 之自同构. 今再施行一个形如 (1) 的映射

$$(x_1, \cdots, x_n) \to (x_1, \cdots, x_n)^{\sigma-1} \left[\begin{pmatrix} T_1 & 0 \\ 0 & 1 \end{pmatrix}^{\sigma-1} \right]^{1},$$

于是得到的新映射就有

$$(x_1, \cdots, x_{n-1}, 0) \to (x_1, \cdots, x_{n-1}, 0).$$

这样一来, 可以和 $n = 2$ 的情形一样去证明, 对 n 维仿射空间中每个点 $(x_1, \cdots, x_n)$ 均有

$$(x_1, \cdots, x_n) \to (x_1, \cdots, x_n).$$

这样定理 1 完全证毕.

没有什么特别困难, 我们可以把定理 1 推广成:

定理 2　设 A_n 为体 K 上的 (左或右)n 维仿射空间, $A'_{n'}$ 为体 K' 上的 (左或右)n' 维仿射空间. 假定有一个从 A_n 到 $A'_{n'}$ 的 1-1 变换将线变到线, 而当 $n \geqslant 3$,

$K = F_2$ 时更将面变到面, 则 $n = n'$ 而 K 与 K' 或者同构或者反同构. 在第一种情形, A_n 和 $A'_{n'}$ 同为左空间或右空间. 如果我们把 K 与 K' 视为同一, 并假定 A_n 和 $A'_{n'}$ 同为左空间, 则变换可表成 (1) 的形状. 在第二种情形, A_n 和 $A'_{n'}$ 中一个是左空间, 另一个是右空间. 假定 A_n 是左空间, $A'_{n'}$ 是右空间, 则变换可表成

$$(6) \qquad (y_1, \cdots, y_n)' = T(x_1, \cdots, x_n)^{\tau'} + (\alpha_1, \cdots, \alpha_n)',$$

其中 τ' 表反同构.

§10 射影几何的基本定理

定理 1 设 $n > 1$, 体 K 上的 n 维射影空间到它自己之上的一个一一对应将线变到线者必为下形:

$$(1) \qquad (x_0, x_1, \cdots, x_n) \to (x_0, x_1, \cdots, x_n)^{\sigma} T,$$

其中 $T = T^{(n+1)}$ 为可逆矩阵, σ 为体 K 之自同构. 而且, 反过来, (1) 形的变换必将线变到线.

【证】 设 $\mathscr{A}$ 为所考虑的变换, 可以证明, 如 $\mathscr{A}$ 将线变到线, 则 $\mathscr{A}$ 必将面变到面. 依定理 7.3, 我们可以假定

$$(2) \qquad \begin{cases} \mathscr{A}(1,0,0,\cdots,0) = (1,0,0,\cdots,0), \\ \mathscr{A}(0,1,0,\cdots,0) = (0,1,0,\cdots,0), \\ \cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots \\ \mathscr{A}(0,\cdots,0,1) = (0,\cdots,0,1), \\ \mathscr{A}(1,\cdots,1) = (1,\cdots,1). \end{cases}$$

于是 $\mathscr{A}$ 将超平面 $x_0 = 0$(它是由点 $(0,1,0,\cdots,0), \cdots, (0,\cdots,0,1)$ 所决定的) 变到它自己, 因之 $\mathscr{A}$ 将有穷点变到有穷点, 即 $\mathscr{A}$ 诱导出由绝对 $x_0 = 0$ 所决定的仿射空间的一个映射, 而这个映射将仿射空间中的线变到线, 同时也将面变到面. 因之, 依定理 9.1, 就有

$$\mathscr{A}(x_0, x_1, \cdots, x_n) = (x_0, x_1, \cdots, x_n)^{\sigma} \begin{pmatrix} 1 & a \\ 0 & A \end{pmatrix},$$

对所有 $(x_0, x_1, \cdots, x_n)$ 而 $x_0 \neq 0$ 的点都成立, 其中 $a = a^{(1,n)}$ 而 $A = A^{(n)}$ 为可逆. 由于 (2), 我们有 $a = 0$, 而 $A = I^{(n)}$. 施行了体的一个自同构以后可以假定

$$(3) \qquad \mathscr{A}(x_0, x_1, \cdots, x_n) = (x_0, x_1, \cdots, x_n)$$

对所有 $(x_0, x_1, \cdots, x_n)$ 而 $x_0 \neq 0$ 的点都成立.

同样有

$$\mathscr{A}(x_0, x_1, \cdots, x_n) = (x_0, x_1, \cdots, x_n)^{\sigma i} \tag{4}$$

对所有 $(x_0, x_1, \cdots, x_n)$ 而 $x_i \neq 0$ 的点都成立. 因 $n > 1$, 比较 (3) 及 (4) 就有

$$\sigma_1 = \sigma_2 = \cdots = \sigma_n = 1,$$

所以

$$\mathscr{A}(x_0, x_1, \cdots, x_n) = (x_0, x_1, \cdots, x_n)$$

对所有 $(x_0, x_1, \cdots, x_n) \neq (0, 0, \cdots, 0)$ 的点都成立. 定理证毕.

应该指出, $n(> 1)$ 维射影几何基本定理的证明比 1 维的容易得多, 这是因为"交与联"的方法不能用于 1 维的情形. 而在 1 维的情形, 调和点列是一个重要概念, 然而, 如果维数高于 1, 调和点列这个性质可以由"交与联"推出来, 即调和点列可以用完全四边形来定义.

我们有下述定理 1 的推广:

定理 2　设 $P_n(K)$ 为一 n 维 (左或右) 射影空间, 而设 $P_{n'}(K')$ 为一 n' 维 (左或右) 射影空间. 如果有 1-1 对应从 $P_n(K)$ 到 $P_{n'}(K')$ 而将线变到线, 则 $n = n'$, 同时 K 与 K' 同构或反同构. 在第一种情形, $P_n(K)$ 和 $P_{n'}(K')$ 同为左空间或同为右空间; 假定它们都是左空间, 则变换可写成 (1) 的形状. 在第二种情形, 一为左空间, 另一为右空间; 假定 $P_n(K)$ 为左空间, 而 $P_{n'}(K')$ 为右空间, 则变换可写成

$$(y_0, y_1, \cdots, y_n)' = T(x_0, x_1, \cdots, x_n)^{\tau'},$$

其中 τ' 表反同构.

§11　有 限 几 何

本节中假定基本域 K 为 $q = p^l$ 个元素的有限域.

定理 1　n 维行向量空间令 q^n 个元素.

此为显然.

定理 2　在 n 维行向量空间中一共有

$$(q^n - 1)(q^n - q) \cdots (q^n - q^{m-1})$$

组线性无关向量组, 每组含 m 个向量.

【证】 用归纳法来证本定理. 因为任何异于 0 的向量必线性无关, 故定理对于 $m=1$ 成立. 假定定理对于 $m-1$ 成立, 则有

$$(q^n-1)(q^n-q)\cdots(q^n-q^{m-2})$$

组线性无关向量组, 每组含 $m-1$ 个向量. 因 m 个线性无关向量可以由一已知 $m-1$ 个线性无关向量组添加一个不属于由这 $m-1$ 个向量所生成的子空间中的向量得到, 而这个子空间一共有 q^{m-1} 个向量, 因之定理对于 m 也成立.

定理 3 n 级一般线性群 $GL_n(K)$ 有

$$(q^n-1)(q^n-q)\cdots(q^n-q^{n-1})$$

个元素, 而 n 级射影一般线性群 $PGL_n(K)$ 有

$$\frac{(q^n-1)(q^n-q)\cdots(q^n-q^{n-1})}{q-1}$$

个元素.

这是上定理的直接推论.

定理 4 $SL_n(K)$ 的元素个数为

$$\frac{(q^n-1)(q^n-q)\cdots(q^n-q^{n-1})}{q-1}.$$

【证】 $GL_n(K)$ 中任一矩阵 A 可唯一分解成

$$A=BD(\mu),$$

其中 $B\in SL_n(K)$ 而 $D(\mu)=[1,\cdots,1,\mu]$, 因而本定理由上定理推得.

定理 5 $PSL_n(K)$ 的阶为

$$\frac{(q^n-1)(q^n-q)\cdots(q^n-q^{n-1})}{d\cdot(q-1)},$$

其中 $d=(q-1,n)$.

【证】 显然, $PSL_n(K)$ 的阶为

$$\frac{(q^n-1)(q^n-q)\cdots(q^n-q^{n-1})}{d'\cdot(q-1)},$$

而 d' 为对角矩阵 λI 的个数而 $\lambda^n=1$. 由 $\lambda^{q-1}=1$ 对于所有 $\lambda(\neq 0)\in K$ 都成立, 可推出 $\lambda^n=1$ 的解的个数等于 $\lambda^d=1$ 的解的个数, 而 $d=(q-1,n)$. 因 $d|(q-1)$, 所以 $\lambda^d=1$ 的解的个数为 d, 故 $d'=d$. 定理得证.

定理 6 n 维射影空间的点的个数为

$$\frac{q^{n+1}-1}{q-1}.$$

【证】 $n+1$ 数组共有 q^{n+1} 个. 除去 $n+1$ 个数都为 0 的那个数组以外共有 $q^{n+1}-1$ 个. 因共有 $q-1$ 个数组同时作为一个点的坐标, 故定理成立.

定理 7 n 维射影空间中 m 维线性子空间的个数为

$$\frac{(q^{n+1}-1)(q^{n+1}-q)\cdots(q^{n+1}-q^m)}{(q^{m+1}-1)(q^{m+1}-q)\cdots(q^{m+1}-q^m)}.$$

【证】 由定理 2, 在 n 维射影空间中, 线性无关点组, 每组含 $m+1$ 个点的个数为

$$(q^{n+1}-1)(q^{n+1}-q)\cdots(q^{n+1}-q^m).$$

这就是秩为 $m+1$ 而型为 $(m+1,n+1)$ 的矩阵的个数. 两个这种矩阵表同一子空间当且仅当它们差一个 $m+1$ 行可逆矩阵. 又依定理 3, $m+1$ 行可逆矩阵的个数为

$$(q^{m+1}-1)(q^{m+1}-q)\cdots(q^{m+1}-q^m),$$

因而定理得证.

注意, 我们附带证明了

$$\frac{(q^{n+1}-1)(q^{n+1}-q)\cdots(q^{n+1}-q^m)}{(q^{m+1}-1)(q^{m+1}-q)\cdots(q^{m+1}-q^m)}$$

是一个整数.

第五章　长方阵几何学

§1　长方阵几何学

设 K 为体, $P^l_{m+n-1}(K)$ 为 K 上的 $m+n-1$ 维的左射影空间. 假定在 $P^l_{m+n-1}(K)$ 中任意取定了一组坐标. 今考虑 $P^l_{m+n-1}(K)$ 中所有 $m-1$ 维线性子空间所成之集合, 这样一个线性子空间由其中任意 m 个线性无关的点

$$(x^i_1, x^i_2, \cdots, x^i_{m+n}) \quad (i=1,2,\cdots,m)$$

确定, 也可以用矩阵

$$W = \begin{pmatrix} x^1_1 & x^1_2 & \cdots & x^1_{m+n} \\ \cdots & \cdots & \cdots & \cdots \\ x^m_1 & x^m_2 & \cdots & x^m_{m+n} \end{pmatrix}$$

表示它, W 是 $(m,m+n)$ 型的, 而且秩为 m. 反之, 任意 $(m,m+n)$ 型而秩 m 的矩阵 $W=(x^i_j)$ 都是点 $(x^i_1,\cdots,x^i_{m+n})(i=1,\cdots,m)$ 所确定的 $m-1$ 维线性子空间的矩阵表示. 两个 $(m,m+n)$ 型而秩 m 的矩阵 W_1 和 W_2 称为等价, 如果有一个可逆矩阵 $Q=Q^{(m)}$, 使

$$W_1 = QW_2.$$

显然, 这是个等价关系. 两个 $(m,m+n)$ 型而秩 m 的矩阵表同一 $m-1$ 维线性子空间当且仅当它们等价. $P^l_{m+n-1}(K)$ 中的 $m-1$ 维线性子空间的全体或 $(m,m+n)$ 型而秩 m 的矩阵等价类的全体称为组成 Grassmann 空间或 $(m,m+n)$ 型矩阵的射影空间. 每个 $m-1$ 维的子空间或每个 $(m,m+n)$ 型而秩 m 的矩阵等价类称为这个空间中的点, 每一 $(m,m+n)$ 型而秩 m 的矩阵就称为这个矩阵所属的那个等价类相应点的坐标. 我们通常为简便计常说"点 W"来代替"W 所表示的点".

显然, 我们的空间中有变换群, 其中元素为

$$W^* = QW^\sigma P, \tag{1}$$

其中 $Q=Q^{(m)}, P=P^{(m+n)}$ 为可逆矩阵, 而 σ 为体 K 之自同构. 这个空间对这个群而言是可迁的. 在这个群之下, 我们空间的几何学称为 Grassmann 几何学或 $(m,m+n)$ 型矩阵的射影几何学. 如果 $m=1$, 这就是通常的射影几何学, 如果 $n=1$, 这就是超平面的几何学, 即通常的射影几何学的对偶.

两个相异的点 W_1 和 W_2 称为粘切, 如果

(2)
$$\begin{pmatrix} W_1 \\ W_2 \end{pmatrix}$$

的秩为 $m+1$. 对于相异的 W_1 和 W_2 来说, $m+1$ 是最小可能的秩值. 实际上, 如果 (2) 的秩为 m, 即因 W_1 的秩为 m, W_2 的每行就是 W_1 诸行的线性组合, 因之

$$W_2 = QW_1,$$

即 W_1 和 W_2 表同一点. 当 $m=1$ 或 $n=1$ 时, 两点粘切当且仅当它们相异.

显然, (1) 不变粘切关系. 因为

$$\begin{pmatrix} W_1^* \\ W_2^* \end{pmatrix} = \begin{pmatrix} Q_1 & \\ & Q_2 \end{pmatrix} \begin{pmatrix} W_1 \\ W_2 \end{pmatrix}^{\sigma} P.$$

$(m, m+n)$ 型矩阵射影几何学的基本问题即为求出空间中所有 1-1 变换使粘切关系不变者. 在本章之末将证明当 $m>1$ 及 $n>1$ 时, 这样一个变换一定是 (1) 的形状; 除非 $m=n$. 如果 $m=n>1$, 则还有另外一类变换, 这在 §2 中要讨论到. 当 $m=1$ 或 $n=1$ 时, 粘切这个条件只是说变换是 1-1 的, 因之, 所有 1-1 变换都不变粘切关系, 所以, 在这种情形, 即通常的射影几何或其对偶的情形, 为了刻画 (1) 所形成的群还需要加上其他条件, 这我们在第二章和第四章中已经作了, 因之, 在本章中我们恒假定 $m>1$ 及 $n>1$.

我们把 W 写成

$$W = (X \quad Y), \quad X = X^{(m,n)}, \quad Y = Y^{(m,m)}.$$

具可逆的 Y 的 W 称为有穷点而其余的点称为无穷远点, 如 W 为有穷点, 则引进

$$Z = Y^{-1}X$$

为 W 的非齐次坐标. 如果 $W^* = (X^*Y^*)$ 和 $W = (X \quad Y)$ 都是有穷点, 则 (1) 式可表成

(3)
$$Z^* = Y^{*-1}X^* = (Z^{\sigma}B + D)^{-1}(Z^{\sigma}A + C),$$

其中

$$P = \begin{pmatrix} A & B \\ C & D \end{pmatrix}, \quad A = A^{(n)}, \quad B = B^{(n,m)}, \quad C = C^{(m,n)}, \quad D = D^{(m)}.$$

两个有穷点 Z 和 Z_1 粘切当且仅当 $Z-Z_1$ 的秩为 1. 事实上, 我们有

$$\begin{aligned}\begin{pmatrix} X & Y \\ X_1 & Y_1 \end{pmatrix} &= \begin{pmatrix} Y & 0 \\ 0 & Y_1 \end{pmatrix} \begin{pmatrix} Z & I \\ Z_1 & I \end{pmatrix} \\ &= \begin{pmatrix} Y & 0 \\ 0 & Y_1 \end{pmatrix} \begin{pmatrix} I & I \\ 0 & I \end{pmatrix} \begin{pmatrix} Z-Z_1 & 0 \\ Z_1 & I \end{pmatrix}\end{aligned}$$

无穷远点之全体组成无穷远流形. 取无穷远流形为绝对, 我们就得到一个几何, 称为 (m,n) 型矩阵的仿射几何. (如果 $m=1$, 即为通常的仿射几何.) 这个几何中的点就是矩阵的射影几何中的有穷点, 因之, 这个几何的空间由所有 (m,n) 型矩阵组成, 这空间称为 (m,n) 型矩阵的仿射空间. 为要求得这个空间的群, 我们来研究 (3). 显然, 只要求得所有可能的 B 和 D 使 $(Z^\sigma B+D)$ 对所有的 Z 可逆即可. 令 $Z=0$ 得出 D 可逆, 因之 $(Z^\sigma BD^{-1}+I)$ 对所有 Z 可逆. 让 Z 取特殊值可得出 $BD^{-1}=0$, 于是 $B=0$. 因之, (3) 变成

$$Z^*=D^{-1}(Z^\sigma A+C),$$

也可以写成

(4) $$Z^*=PZ^\sigma Q+R,$$

其中 $P=P^{(m)},Q=Q^{(n)}$ 为可逆矩阵. 所有这种形状的变换组成一群, 即 (m,n) 型矩阵的仿射几何学的群.

定理 1 $(m,m+n)$ 型矩阵的射影空间中任何一对相互粘切的点可以同时在群 (1) 之下化到

$$(0\ \ I^{(m)})\quad 和\quad (N\ \ I^{(m)}),$$

而

$$N=\begin{pmatrix}1&0&\cdots&0\\0&0&\cdots&0\\\vdots&\vdots&&\vdots\\0&0&\cdots&0\end{pmatrix}.$$

【证】 因空间可迁, 故可假定其中一点为

$$(0\ \ I^{(m)}),$$

将另一点的坐标写成

(5) $$(X^{(m,n)}\ \ Y^{(m)}),$$

则 X 的秩为 1, 因之有可逆矩阵 $Q=Q^{(m)}$ 和 $P=P^{(n)}$ 存在, 使

$$QXP=N.$$

于是

$$Q(X\ \ Y)\begin{pmatrix}P&0\\0&I\end{pmatrix}=(N\ \ QY),$$

$$(0\ \ I)\begin{pmatrix}P&0\\0&I\end{pmatrix}=(0\ \ I),$$

因之, 我们可以假定 (5) 中的 $X = N$.

如 Y 可逆, 则

$$(N \quad Y)\begin{pmatrix} I & 0 \\ 0 & Y^{-1} \end{pmatrix} = (N \quad I),$$

$$Y(0 \quad I)\begin{pmatrix} I & 0 \\ 0 & Y^{-1} \end{pmatrix} = (0 \quad I),$$

此时定理得证.

如 Y 不可逆, 则因 $(N \quad Y)$ 之秩为 m, 若将 Y 写作

$$Y = \begin{pmatrix} y_1 \\ y_2 \\ \vdots \\ y_m \end{pmatrix},$$

则其中 $y_2, \cdots, y_m$ 必线性无关, 于是可求得向量 z, 使

$$\begin{pmatrix} z + y_1 \\ y_2 \\ \vdots \\ y_m \end{pmatrix}$$

之秩为 m. 令

$$C = \begin{pmatrix} z \\ 0 \\ \vdots \\ 0 \end{pmatrix},$$

则

$$(0 \quad I)\begin{pmatrix} I & C \\ 0 & I \end{pmatrix} = (0 \quad I),$$

$$(N \quad Y)\begin{pmatrix} I & C \\ 0 & I \end{pmatrix} = (N \quad NC + Y),$$

而 $NC + Y$ 可逆, 就化为上述情形, 故定理得证.

§2 方阵几何学

当 $m = n$ 时, 有一类非齐次变换

(1) $$Z^* = (Z^{\tau'}B + D)^{-1}(Z^{\tau'}A + C),$$
其中 τ' 为 K 的反自同构, 如果 K 确有反自同构的话. 在这类变换中最重要的一个是

(2) $$Z^* = Z^{\tau'}.$$

如果引进齐次坐标, 我们有

$$Y^{*-1}X^* = X^{\tau'}(Y^{\tau'})^{-1},$$

即

$$X^*Y^{\tau'} = Y^*X^{\tau'}.$$

我们可将这个关系写成

(3) $$(X^* \quad Y^*)\mathfrak{F}(X \quad Y)^{\tau'} = 0,$$
其中

$$\mathfrak{F} = \begin{pmatrix} 0 & I \\ -I & 0 \end{pmatrix}.$$

现在我们来证明 (3) 定义了方阵射影空间中一个一对一的变换. 令 $(X_1 \quad Y_1)$ 为另一点适合

$$(X_1 \quad Y_1)\mathfrak{F}(X \quad Y)^{\tau'} = 0,$$

则

$$\begin{pmatrix} X^* & Y^* \\ X_1 & Y_1 \end{pmatrix}\mathfrak{F}(X \quad Y)^{\tau'} = 0,$$

依 Sylevester 的 nullity 定理就有

$$\begin{pmatrix} X^* & Y^* \\ X_1 & Y_1 \end{pmatrix}$$

之秩 $\leqslant n$. 因为 $(X^* \quad Y^*)$ 和 $(X \quad Y)$ 之秩皆为 n, 故存在非奇异矩阵 Q, 使得

$$(X^* \quad Y^*) = Q(X \quad Y),$$

即 $(X^* \quad Y^*)$ 和 $(X_1 \quad Y_1)$ 表同一点.

一般言之, 令 R 表 $2n$ 行的可逆矩阵, 则

(4) $$(X^* \quad Y^*)R(X \quad Y)\tau' = 0$$
就定义了一个方阵射影空间中的一一变换, 这是 (1) 的齐次形式.

两个形状 (4) 的变换之积为 §1 中形状 (1) 的变换, 实际上, 令

$$(X^* \quad Y^*)R_1(X \quad Y)^{\tau_1'} = 0,$$
$$(X^{**} \quad Y^{**})R_2(X^* \quad Y^*)^{\tau_2'} = 0$$

为两个形如 (4) 的变换, 则 $\sigma=\tau_1\tau_2$ 为体之自同构. 行施 τ_2' 到第一个式子就得出

$$(X\ \ Y)^{\sigma}R_1^{\tau_2'}(X^*\ \ Y^*)^{\tau_2'}=0.$$

将这个关系式与第二个变换合并就有

$$\begin{pmatrix}(X\ \ Y)^{\sigma}R_1^{\tau_2'}\\(X^{**}\ \ Y^{**})R_2\end{pmatrix}(X^*\ \ Y^*)^{\tau_2'}=0.$$

依 Sylevester 的 nullity 定理就有

$$(X^{**}\ \ Y^{**})R_2=Q(X\ \ Y)^{\sigma}R_1^{\tau_2'},$$

因之

$$(X^{**}\ \ Y^{**})=Q(X\ \ Y)^{\sigma}R_1^{\tau_2'}R_2^{-1}.$$

这是 §1 形状 (1) 的一个变换.

这就证明了下面的定理:

定理 1　由 §1 形状 (1) 的变换和本节形状 (4) 的变换所生成的群也就是由 §1 形状 (1) 的变换及一个本节形状 (4) 的变换, 例如 (3) 所生成的.

现在我们要证明这个扩大了的群不变粘切关系.

定理 2　变换 (4) 不变粘切关系. 确切地说, 设 $(X\ \ Y)$ 和 $(X_1\ \ Y_1)$ 为一对互相粘切的点, 令

$$(X^*\ \ Y^*)R(X\ \ Y)^{\tau'}=0,$$
$$(X_1^*\ \ Y_1^*)R(X_1\ \ Y_1)^{\tau'}=0,$$

则 $(X^*\ \ Y^*)$ 和 $(X_1^*\ \ Y_1^*)$ 仍是一对互相粘切的点.

【证】　依定理 1.1, 我们有一个形状

$$(X\ \ Y)=Q(U\ \ V)P$$

的变换将 $(0\ \ I)$ 和 $(N\ \ I)$ 分别变到 $(X\ \ Y)$ 和 $(X_1\ \ Y_1)$. 令

$$(U^*\ \ V^*)=(X^*\ \ Y^*)RP^{\tau'}$$

及

$$(U_1^*\ \ V_1^*)=(X_1^*\ \ Y_1^*)RP^{\tau'},$$

则

$$(U^*\ \ V^*)(0\ \ I)^{\tau'}=0$$

及

$$(U_1^* \quad V_1^*)(N \quad I)^{\tau'} = 0.$$

因之

$$V^* = 0, \quad U_1^* N + V_1^* = 0,$$

于是

$$\begin{pmatrix} U^* & V^* \\ U_1^* & V_1^* \end{pmatrix} = \begin{pmatrix} U^* & 0 \\ U_1^* & -U_1^* N \end{pmatrix}$$

的秩 $\leqslant n+1$. 因之

$$\begin{pmatrix} X^* & Y^* \\ X_1^* & Y_1^* \end{pmatrix}$$

的秩 $\leqslant n+1$. 因为 (4) 是一一的, $(X^* \quad Y^*)$ 和 $(X_1^* \quad Y_1^*)$ 为不同的点, 所以

$$\begin{pmatrix} X^* & Y^* \\ X_1^* & Y_1^* \end{pmatrix}$$

的秩恰为 $n+1$, 即 $(X^* \quad Y^*)$ 和 $(X_1^* \quad Y_1^*)$ 粘切.

【备注】 采用非齐次坐标, 我们有变换

$$Z^* = (Z^\sigma B + D)^{-1}(Z^\sigma A + C)$$

及

$$Z^* = (Z^{\tau'} B + D)^{-1}(Z^{\tau'} A + C).$$

表面上, 计算两个这种变换的乘积好像很困难, 但这个困难可以借助于以下等式克服之. 对任意 $Z = Z^{(n)}$,

$$(ZB + D)^{-1}(ZA + C) = (SZ - R)(-QZ + P)^{-1},$$

其中

$$\begin{pmatrix} A & B \\ C & D \end{pmatrix}\begin{pmatrix} P & Q \\ R & S \end{pmatrix} = \begin{pmatrix} I & 0 \\ 0 & I \end{pmatrix}.$$

§3 算术距离

定义 1 在长方阵的射影空间中两个不同的点 W_0 和 W_r 的算术距离称为 r, 如果有 $r-1$ 个点 $W_1, W_2, \cdots, W_{r-1}$ 存在, 使得 W_i 和 $W_{i-1}(1 \leqslant i \leqslant r)$ 粘切而 r 是具有此性质的最小正整数.

如果 W_0 和 W_r 的算术距离为 r, 我们写 $d(W_0,W_r)=r$. 如果 W_0 与 W_r 重合, 我们约定 $d(W_0,W_r)=0$. 显然, 我们有以下诸性质:

Ⅰ. $d(W_1,W_2)=0$ 当且仅当 $W_1=QW_2$;

Ⅱ. $d(W_1,W_2)=d(W_2,W_1)$;

Ⅲ. $d(W_1,W_2)+d(W_2,W_3)\geqslant d(W_1,W_3)$.

而且由定义立刻推得长方阵射影空间中的 1-1 变换使粘切不变者也使算术距离不变.

定理 1　长方阵射影空间中两点 W_0 和 W_r 的算术距离为 r, 当且仅当

$$\begin{pmatrix} W_0 \\ W_r \end{pmatrix}$$

的秩为 $m+r$.

【证】　如果 $\begin{pmatrix} W_0 \\ W_r \end{pmatrix}$ 的秩为 $m+r$, 则像在定理 1.1 的证明一样, 我们可以用 §1 中形式 (1) 的一个变换把 W_0 和 W_r 分别变到

$$(0\ \ I^{(m)})\quad 和\quad \left(\begin{pmatrix} I^{(r)} & 0 \\ 0 & 0 \end{pmatrix} I^{(m)}\right).$$

因之, 不失普遍性, 我们可以假定

$$W_0=(0\ \ I^{(m)})\quad 和\quad W_r=\left(\begin{pmatrix} I^{(r)} & 0 \\ 0 & 0 \end{pmatrix} I^{(m)}\right),$$

于是

$$W_i=\left(\begin{pmatrix} I^{(i)} & 0 \\ 0 & 0 \end{pmatrix} I^{(m)}\right)\quad (1\leqslant i\leqslant r-1)$$

就是 W_0 和 W_r 之间的 $r-1$ 个中间点而任意相邻两点皆粘切, 所以

$$d(W_0,W_r)\leqslant r.$$

反之, 如果 $d(W_0,W_r)=r$, 则由关于矩阵的秩的一个著名定理可得

$$\operatorname{rank}\begin{pmatrix} W_0 \\ W_r \end{pmatrix}\leqslant \operatorname{rank}\begin{pmatrix} W_0 \\ W_i \end{pmatrix}+\operatorname{rank}\begin{pmatrix} W_i \\ W_r \end{pmatrix}-m,$$

对于秩为 m 的矩阵 W_0, W_i 和 W_r. 于是我们有

$$\begin{aligned}\operatorname{rank}\begin{pmatrix} W_0 \\ W_r \end{pmatrix} &\leqslant \operatorname{rank}\begin{pmatrix} W_0 \\ W_1 \end{pmatrix} + \operatorname{rank}\begin{pmatrix} W_1 \\ W_2 \end{pmatrix} + \cdots \\ &\quad + \operatorname{rank}\begin{pmatrix} W_{r-1} \\ W_r \end{pmatrix} - (r-1)m \\ &= r(m+1) - (r-1)m = m + r. \end{aligned}$$

因而定理得证.

如果 $W_0 = (X_0 \ \ Y_0)$ 和 $W_r = (X_r \ \ Y_r)$ 为有穷点, 我们可以引进非齐次坐标 $Z_0 = Y_0^{-1}X_0$ 和 $Z_r = Y_r^{-1}X_r$, 于是它们的算术距离为 r, 当且仅当 $Z_0 - Z_r$ 的秩为 r. 事实上, 我们有

$$\begin{pmatrix} X_0 & Y_0 \\ X_r & Y_r \end{pmatrix} = \begin{pmatrix} Y_0 & 0 \\ 0 & Y_r \end{pmatrix} \begin{pmatrix} I & I \\ 0 & I \end{pmatrix} \begin{pmatrix} Z_0 - Z_r & 0 \\ Z_r & I \end{pmatrix}$$

在长方阵仿射空间中, 我们有以下类似的定义.

定义 2 长方阵仿射空间中两个不同的点 Z_0 和 Z_r 的算术距离称为 r, 如果有 $r-1$ 个点 $Z_1, Z_2, \cdots, Z_{r-1}$, 使得 Z_i 和 $Z_{i-1} (1 \leqslant i \leqslant r)$ 粘切, 而 r 是具此性质的最小正整数.

然后, 我们可以证明

定理 2 长方阵仿射空间中两点 Z_0 和 Z_r 的算术距离为 r, 当且仅当 $Z_0 - Z_r$ 的秩为 r.

§4 长方阵仿射空间中秩为 1 的极大集

在 §4 ~ §7 中我们仅研究长方阵仿射空间, 因之, 我们有时把“长方阵仿射空间”这句话省去不说.

定义 长方阵仿射空间中的一个秩为 1 的极大集是其中的一个点集, 具有性质:

Ⅰ. 其中任意两点皆粘切;

Ⅱ. 与此集中一切点粘切的点必属于此集.

定理 1 任意秩为 1 的极大集在 §1 形式 (4) 的变换之下必与由下列元素所组成的秩为 1 的极大集等价:

(1)
$$\begin{pmatrix} x_1 & x_2 & \cdots & x_n \\ 0 & 0 & \cdots & 0 \\ \vdots & & & \\ 0 & 0 & \cdots & 0 \end{pmatrix},$$

其中 $x_1, x_2, \cdots, x_n$ 独立地跑过 K, 或者与由下列元素所组成的秩为 1 的极大集等价：

$$(2) \qquad \begin{pmatrix} y_1 & 0 & \cdots & 0 \\ y_2 & 0 & \cdots & 0 \\ \vdots & \vdots & & \\ y_m & 0 & \cdots & 0 \end{pmatrix},$$

其中 $y_1, y_2, \cdots, y_m$ 独立地跑过 K.

【证】 我们可以假定这个秩为 1 的极大集包有 0 和

$$Z_0 = \begin{pmatrix} 1 & 0 & \cdots & 0 \\ 0 & 0 & \cdots & 0 \\ \cdots & \cdots & \cdots & \cdots \\ 0 & 0 & \cdots & 0 \end{pmatrix}.$$

令 Z 为此集中任意一点 $(\neq 0, Z_0)$. 因 Z 与 0 粘切, 故 Z 之秩为 1, 因之我们有

$$Z = \begin{pmatrix} a_1b_1 & \cdots & a_1b_n \\ \cdots & \cdots & \cdots \\ a_mb_1 & \cdots & a_mb_n \end{pmatrix}.$$

因为 $Z - Z_0$ 之秩为 1, 我们有

$$a_ib_j = 0 \quad (2 \leqslant i \leqslant m, 2 \leqslant j \leqslant n).$$

如果 $a_2, a_3, \cdots, a_m$ 不全为 0, 我们必有 $b_2 = b_3 = \cdots = b_n = 0$, 即

$$(3) \qquad Z = \begin{pmatrix} a_1b_1 & 0 & \cdots & 0 \\ a_2b_1 & 0 & \cdots & 0 \\ \vdots & & & \\ a_mb_1 & 0 & \cdots & 0 \end{pmatrix}.$$

否则, 我们有

$$(4) \qquad Z = \begin{pmatrix} a_1b_1 & a_1b_2 & \cdots & a_1b_n \\ 0 & 0 & \cdots & 0 \\ \vdots & & & \\ 0 & 0 & \cdots & 0 \end{pmatrix}.$$

以下形状的元素：

$$(5)\qquad \begin{pmatrix} \alpha & 0 & \cdots & 0 \\ 0 & 0 & \cdots & 0 \\ \vdots & & & \\ 0 & 0 & \cdots & 0 \end{pmatrix}.$$

显然不能组成一个秩为 1 的极大集. 如果所给的秩为 1 的极大集中包有 (5) 以外的一个元素, 这个元素或为 (3) 的形状, 或为 (4) 的形状. 这就是说, 包有 0 和 Z_0 的秩为 1 的极大集或为 (1) 或为 (2).

以上证明也使我们得到

定理 2 给了任意两个互相粘切的点, 有且仅有两个秩为 1 的极大集包有它们.

更进一步, 我们有

定理 3 有唯一的一个公共点的两个秩为 1 的极大集在 §1 形式 (4) 的变换之下可以变到下面这两个秩为 1 的极大集:

$$\begin{pmatrix} x_{11} & \cdots & x_{1n} \\ 0 & \cdots & 0 \\ \vdots & & \\ 0 & \cdots & 0 \end{pmatrix}, \quad \begin{pmatrix} 0 & \cdots & 0 \\ x_{21} & \cdots & x_{2n} \\ 0 & \cdots & 0 \\ \vdots & & \\ 0 & \cdots & 0 \end{pmatrix},$$

而 $x_{ij}(i=1,2;j=1,2,\cdots,n)$ 独立地跑过 K; 或者变到下面这两个秩为 1 的极大集:

$$\begin{pmatrix} y_{11} & 0 & \cdots & 0 \\ y_{21} & 0 & \cdots & 0 \\ \vdots & \vdots & & \\ y_{m1} & 0 & \cdots & 0 \end{pmatrix}, \quad \begin{pmatrix} 0 & y_{12} & 0 & \cdots & 0 \\ 0 & y_{22} & 0 & \cdots & 0 \\ \vdots & \vdots & \vdots & & \\ 0 & y_{m2} & 0 & \cdots & 0 \end{pmatrix},$$

而 $y_{ij}(i=1,2,\cdots,m;j=1,2)$ 独立地跑过 K.

【证】 不失普遍性, 我们可以假定公共点变到了 0 而其中某一个秩为 1 的极大集变到了

$$\begin{pmatrix} x_{11} & \cdots & x_{1n} \\ 0 & \cdots & 0 \\ \vdots & & \\ 0 & \cdots & 0 \end{pmatrix}$$

(由于相似性, 我们省去另一情形的讨论).

令

$$Z = \begin{pmatrix} a_{11} & \cdots & a_{1n} \\ \multicolumn{3}{c}{\dotfill} \\ a_{m1} & \cdots & a_{mn} \end{pmatrix}$$

为另一个秩为 1 的极大集中之非零点, 则我们有可逆矩阵 $P^{(m-1)}$ 及 $Q^{(n)}$ 存在, 使得

$$\begin{pmatrix} 1 & 0 \\ 0 & P^{(m-1)} \end{pmatrix} ZQ^{(n)} = \begin{pmatrix} c_1 & c_2 & \cdots & c_n \\ 1 & 0 & \cdots & 0 \\ 0 & 0 & \cdots & 0 \\ \vdots & & & \\ 0 & 0 & \cdots & 0 \end{pmatrix}.$$

因其秩为 1, 故 $c_2 = c_3 = \cdots = c_n = 0$(任意这样一个变换不变第一个秩为 1 的极大集). 于是变换

$$Z^* = \begin{pmatrix} 1 & -c_1 & 0 & \cdots & 0 \\ 0 & 1 & 0 & \cdots & 0 \\ 0 & 0 & 1 & \cdots & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & 0 & \cdots & 1 \end{pmatrix} Z.$$

就不变第一个秩为 1 的极大集而将上面那个点变到了

$$\begin{pmatrix} 0 & 0 & \cdots & 0 \\ 1 & 0 & \cdots & 0 \\ 0 & 0 & \cdots & 0 \\ \multicolumn{4}{c}{\dotfill} \\ 0 & 0 & \cdots & 0 \end{pmatrix}.$$

这个点和 0 所张成的秩为 1 的极大集为

$$\begin{pmatrix} 0 & 0 & \cdots & 0 \\ x_{21} & x_{22} & \cdots & x_{2n} \\ 0 & 0 & \cdots & 0 \\ \multicolumn{4}{c}{\dotfill} \\ 0 & 0 & \cdots & 0 \end{pmatrix}.$$

或

$$\begin{pmatrix} y_{11} & 0 & \cdots & 0 \\ y_{21} & 0 & \cdots & 0 \\ \vdots & \multicolumn{3}{c}{\cdots\cdots\cdots} \\ y_{m1} & 0 & \cdots & 0 \end{pmatrix}$$

因第一个秩为 1 的极大集和第二个秩为 1 的极大集的交只可能有一点公共, 因之第二种情形不可能, 于是定理得证.

§5 两个秩为 1 的极大集的交集

现在让我们来研究两个秩为 1 的极大集的交集, 假定它们的交集是非空的. 我们可以取 0 作为它们的公共点之一. 包有 0 的极大集必为下列二形状之一:

$$P\begin{pmatrix} x_1 & x_2 & \cdots & x_n \\ 0 & 0 & \cdots & 0 \\ \multicolumn{4}{c}{\cdots\cdots\cdots\cdots\cdots\cdots} \\ 0 & 0 & \cdots & 0 \end{pmatrix}Q$$

或

$$P\begin{pmatrix} y_1 & 0 & \vdots & 0 \\ y_2 & 0 & \vdots & 0 \\ \vdots & \vdots & \vdots & \vdots \\ y_m & 0 & \vdots & 0 \end{pmatrix}Q,$$

其中 $P=P^{(m)}$ 及 $Q=Q^{(n)}$ 为可逆矩阵. 实际上, 设 Z 为秩 1 的一点, 则我们有 P 和 Q, 使得

$$P^{-1}ZQ^{-1}=\begin{pmatrix} 1 & 0 & \cdots & 0 \\ 0 & 0 & \cdots & 0 \\ \multicolumn{4}{c}{\cdots\cdots\cdots\cdots} \\ 0 & 0 & \cdots & 0 \end{pmatrix}.$$

根据定理 4.1 的结果, 断言即得证. 因之我们可以假定这两个秩为 1 的极大集为下列四者之一:

I. $$\begin{pmatrix} x_1 & x_2 & \cdots & x_n \\ 0 & 0 & \cdots & 0 \\ \multicolumn{4}{c}{\cdots\cdots\cdots\cdots\cdots\cdots} \\ 0 & 0 & \cdots & 0 \end{pmatrix} P\begin{pmatrix} y_1 & y_2 & \cdots & y_n \\ 0 & 0 & \cdots & 0 \\ \multicolumn{4}{c}{\cdots\cdots\cdots\cdots\cdots\cdots} \\ 0 & 0 & \cdots & 0 \end{pmatrix}Q,$$

$$\text{II.}\qquad \begin{pmatrix} x_1 & x_2 & \cdots & x_n \\ 0 & 0 & \cdots & 0 \\ \cdots & \cdots & \cdots & \cdots \\ 0 & 0 & \cdots & 0 \end{pmatrix} P \begin{pmatrix} y_1 & 0 & \cdots & 0 \\ y_2 & 0 & \cdots & 0 \\ \vdots & \vdots & & \\ y_m & 0 & \cdots & 0 \end{pmatrix} Q,$$

$$\text{III.}\qquad \begin{pmatrix} x_1 & 0 & \cdots & 0 \\ x_2 & 0 & \cdots & 0 \\ \vdots & \vdots & & \\ x_m & 0 & \cdots & 0 \end{pmatrix} P \begin{pmatrix} y_1 & y_2 & \cdots & y_n \\ 0 & 0 & \cdots & 0 \\ \cdots & \cdots & \cdots & \cdots \\ 0 & 0 & \cdots & 0 \end{pmatrix} Q,$$

$$\text{IV.}\qquad \begin{pmatrix} x_1 & 0 & \cdots & 0 \\ x_2 & 0 & \cdots & 0 \\ \vdots & \vdots & & \\ x_m & 0 & \cdots & 0 \end{pmatrix} P \begin{pmatrix} y_1 & 0 & \cdots & 0 \\ y_2 & 0 & \cdots & 0 \\ \vdots & \vdots & & \\ y_m & 0 & \cdots & 0 \end{pmatrix} Q.$$

第 I 种情形与第 IV 种情形可类似讨论, 而第 II 种情形与第 III 种情形可类似讨论.

我们先来讨论情形 I. 不失普遍性, 我们可以假定 $Q = I$. 设

$$P = (p_{ij}) \quad (1 \leqslant i, j \leqslant m),$$

则立即由适合条件

$$(p_{21}, \cdots, p_{m1})'(y_1, \cdots, y_n) = 0$$

的点 $(y_1, \cdots, y_n)$ 给出: 如果 $(p_{21}, \cdots, p_{m1})$ 为零向量, 则两个秩为 1 的极大集完全相等. 如果 $(p_{21}, \cdots, p_{m1})$ 不是零向量, 则 $(y_1, \cdots, y_n)$ 必须为零向量, 于是这样两个秩为 1 的极大集只有一点公共.

再讨论情形III. 变换 $Z^* = P^{-1}Z$ 将III中的两个秩为 1 的极大集仍变为III中形式的两个, 但 $P = I$, $Q = I$. 因之, 这样两个秩为 1 的极大集之交为

$$\begin{pmatrix} x & 0 & \cdots & 0 \\ 0 & 0 & \cdots & 0 \\ \cdots & \cdots & \cdots & \cdots \\ 0 & 0 & \cdots & 0 \end{pmatrix}, \tag{1}$$

其中 x 跑过 K.

因此我们证明了

定理 1　两个不相同的秩为 1 的极大集的交集或为空或为一点或为一集, 它在 §1 形式 (4) 的变换之下与 (1) 等价.

我们来定义

定义 两个秩为 1 的极大集如公共点不止一点, 则其交称为线, 或确切地说, 秩为 1 的极大集中的线.

定理 2 设 Z_0 和 Z_1 为一对粘切矩阵, 则有一线通过它们.

【证】 不失普遍性, 我们可以假定

$$Z_0 = 0, \quad Z_1 = \begin{pmatrix} 1 & 0 & \cdots & 0 \\ 0 & 0 & \cdots & 0 \\ \cdots & \cdots & \cdots & \cdots \\ 0 & 0 & \cdots & 0 \end{pmatrix}.$$

依定理 4.2, 有两个秩为 1 的极大集包有它们, 它们是 (4.1) 和 (4.2). 这两个秩为 1 的极大集的交集为

$$\begin{pmatrix} t & 0 & \cdots & 0 \\ 0 & 0 & \cdots & 0 \\ \cdots & \cdots & \cdots & \cdots \\ 0 & 0 & \cdots & 0 \end{pmatrix} \quad (t \in K).$$

因之定理得证.

线的一般方程可以表为

$$p'tq + R,$$

其中 p 和 q 分别为 m 维和 n 维向量. 再者, 秩为 1 的极大集 (4.1) 中线的一般方程为

$$t\begin{pmatrix} a_1 & a_2 & \cdots & a_n \\ 0 & 0 & \cdots & 0 \\ \cdots & \cdots & \cdots & \cdots \\ 0 & 0 & \cdots & 0 \end{pmatrix} + \begin{pmatrix} b_1 & b_2 & \cdots & b_n \\ 0 & 0 & \cdots & 0 \\ \cdots & \cdots & \cdots & \cdots \\ 0 & 0 & \cdots & 0 \end{pmatrix},$$

而秩为 1 的极大集 (4.2) 中线的一般方程为

$$\begin{pmatrix} a_1 & 0 & \cdots & 0 \\ a_2 & 0 & \cdots & 0 \\ \vdots & \vdots & & \\ a_m & 0 & \cdots & 0 \end{pmatrix} t + \begin{pmatrix} b_1 & 0 & \cdots & 0 \\ b_2 & 0 & \cdots & 0 \\ \cdots & \cdots & \cdots & \cdots \\ b_m & 0 & \cdots & 0 \end{pmatrix}.$$

§6 长方阵仿射空间中秩为 2 的极大集

定义 设 $m, n > 1$. (m, n) 型长方阵仿射空间中一个点集 M 称为一个秩为 2 的极大集, 如果

I. M 包有两个仅有一个公共点的秩为 1 的极大集, 这公共点称为特殊点, 记作 A. 记这两个秩为 1 的极大集为 M_1, M_2;

II. 所有与 A 的算术距离为 2, 与 M_1 及 M_2 中的点的算术距离 $\leqslant 2$, 而不与 M_1 中所有的点的算术距离都等于 2, 及不与 M_2 中所有的点的算术距离都等于 2 的点皆属于 M, 这种点的集合记作 N;

III. 所有与 A 的算术距离为 1, 与 N 中的点的算术距离 $\leqslant 2$ 而不与 N 中所有的点的算术距离都 $= 2$ 的点都属于 M;

IV. M 不包含其他的点.

我们知道, (m, n) 型长方阵仿射空间中的一个一一变换, 如不变粘切关系, 则也不变算术距离, 因而必将秩为 2 的极大集变为秩为 2 的极大集.

定理 1 任何一个秩为 2 的极大集, 在变换

$$Z^* = PZQ + R \tag{1}$$

之下, 等价于如下的秩为 2 的极大集:

$$\begin{pmatrix} x_{11} & x_{12} & \cdots & x_{1n} \\ x_{21} & x_{22} & \cdots & x_{2n} \\ 0 & 0 & \cdots & 0 \\ \cdots & \cdots & \cdots & \cdots \\ 0 & 0 & \cdots & 0 \end{pmatrix}, \tag{2}$$

其中 $x_{ij}(i = 1, 2; j = 1, 2, \cdots, n)$ 独立地跑过 K, 或者

$$\begin{pmatrix} y_{11} & y_{12} & 0 & \cdots & 0 \\ y_{21} & y_{22} & 0 & \cdots & 0 \\ \vdots & \vdots & \vdots & & \\ y_{m1} & y_{m2} & 0 & \cdots & 0 \end{pmatrix}, \tag{3}$$

其中 $y_{ij}(i = 1, 2, \cdots, m; j = 1, 2)$ 独立地跑过 K.

【证】 依定理 4.3, 不妨设给定的秩为 2 的极大集 M 的特殊点 A 为 0, 并设其中两个仅以 A 为公共点的秩为 1 的极大集为

$$M_1 = \left\{ \begin{pmatrix} x_{11} & x_{12} & \cdots & x_{1n} \\ 0 & 0 & \cdots & 0 \\ \cdots & \cdots & \cdots & \cdots \\ 0 & 0 & \cdots & 0 \end{pmatrix} \middle| x_{1j}\text{跑过}K, j = 1, \cdots, n \right\}$$

及

$$M_2=\left\{\left.\begin{pmatrix}0&0&\cdots&0\\x_{21}&x_{22}&\cdots&x_{2n}\\0&0&\cdots&0\\\multicolumn{4}{c}{\cdots\cdots\cdots\cdots}\\0&0&\cdots&0\end{pmatrix}\right| x_{2j}\text{跑过}K,j=1,\cdots,n\right\}$$

(由于另一情形的讨论相仿, 因而略去). 这样 M 中每个矩阵的秩均 $\leqslant 2$. 若 $m=2$, 定理显然成立. 以下设 $m\geqslant 3$.

设

$$X=\begin{pmatrix}x_{11}&x_{12}&\cdots&x_{1n}\\x_{21}&x_{22}&\cdots&x_{2n}\\\multicolumn{4}{c}{\cdots\cdots\cdots\cdots}\\x_{m1}&x_{m2}&\cdots&x_{mn}\end{pmatrix}=\begin{pmatrix}x_1\\x_2\\\vdots\\x_m\end{pmatrix}$$

为 N 中任一点. 因为 X 与 M_1 中每个点的算术距离都 $\leqslant 2$, 而又不与 M_1 中每个点的算术距离均 $=2$, 故如下 $(m-1)\times n$ 型矩阵:

$$\begin{pmatrix}x_2\\\vdots\\x_m\end{pmatrix}$$

的秩 $=1$. 同样矩阵

$$\begin{pmatrix}x_1\\x_3\\\vdots\\x_m\end{pmatrix}$$

的秩也 $=1$. 如果有某个 $x_i\neq(0,\cdots,0)(3\leqslant i\leqslant m)$, 则有

$$x_k=\lambda_k x_i\quad(\lambda_k\in K;k=1,\cdots,m).$$

这样一来, X 的秩必 $=1$, 与假设矛盾. 所以 $x_i=(0,\cdots,0)(i=3,\cdots,m)$. 这就是说, X 具有形状 (2), 再依性质 II 知一切形状如 (2) 且秩为 2 的矩阵皆包于 M 中.

设 X 是与 0 的算术距离为 1, 与 N 中所有点的算术距离皆 $\leqslant 2$, 而又不与 N

中每个点的算术距离都 $=2$ 的一个点. 写

$$X=\begin{pmatrix} x_1 \\ x_2 \\ \vdots \\ x_m \end{pmatrix}.$$

我们证明 $x_i=0(i=3,\cdots,m)$. 事实上, 假定 $x_3\neq 0$, 则 $x_i=\lambda_i x_3(i=1,2,\cdots,m)$. 于是对于 M 施行如下映射:

$$Z^*=\begin{pmatrix} 1 & 0 & -\lambda_1 & 0 & \cdots & 0 \\ 0 & 1 & -\lambda_2 & 0 & \cdots & 0 \\ 0 & 0 & 1 & 0 & \cdots & 0 \\ 0 & 0 & -\lambda_4 & 1 & \ddots & \vdots \\ 0 & 0 & -\lambda_5 & 0 & \ddots & 0 \\ \cdots & \cdots & \cdots & \vdots & \ddots & \\ 0 & 0 & -\lambda_m & 0 & \cdots\ 0 & 1 \end{pmatrix} Z,$$

则它将 X 映到

$$\overline{X}=\begin{pmatrix} 0 \\ 0 \\ x_3 \\ 0 \\ \vdots \\ 0 \end{pmatrix},$$

而将 M_1,M_2 和 N 映到它们自身之中. 由于 $\overline{X}$ 与 N 中每个点的算术距离皆 $\geqslant 2$, 矛盾, 这样, X 必为形状 (2).

因此, M 由一切形如 (2) 的矩阵组成, 定理证毕.

根据定理 1, 每个秩为 2 的极大集可设为

$$(4)\qquad P\begin{pmatrix} x_{11} & x_{12} & \cdots & x_{1n} \\ x_{21} & x_{22} & \cdots & x_{2n} \\ 0 & 0 & \cdots & 0 \\ \cdots & \cdots & \cdots & \cdots \\ 0 & 0 & \cdots & 0 \end{pmatrix} Q+R\quad (x_{ij}\text{独立地跑过}K),$$

或者

(5) $$P\begin{pmatrix} y_{11} & y_{12} & 0 & \cdots & 0 \\ y_{21} & y_{22} & 0 & \cdots & 0 \\ \cdots & \cdots & \cdots & \cdots & \cdots \\ y_{m1} & y_{m2} & 0 & \cdots & 0 \end{pmatrix} Q + R \quad (y_{ij}\text{独立地跑过}K).$$

我们进而研究一个秩为 1 的极大集与一个秩为 2 的极大集的交集. 假设它们的交集非空, 并且包有秩为 2 的极大集的特殊点. 设这个特殊点为 0. 于是包有 0 的秩为 1 的极大集必为下列形状之一:

(6) $$P\begin{pmatrix} x_{11} & x_{12} & \cdots & x_{1n} \\ 0 & 0 & \cdots & 0 \\ \cdots & \cdots & \cdots & \cdots \\ 0 & 0 & \cdots & 0 \end{pmatrix} Q,$$

或者

(7) $$P\begin{pmatrix} y_{11} & 0 & \cdots & 0 \\ y_{21} & 0 & \cdots & 0 \\ \vdots & \vdots & & \vdots \\ y_{m1} & 0 & \cdots & 0 \end{pmatrix} Q,$$

其中 $P = P^{(m)}$, $Q = Q^{(n)}$ 均为可逆矩阵. 而以 0 为特殊点的秩为 2 的极大集必为下列形状之一:

(8) $$R\begin{pmatrix} x_{11} & x_{12} & \cdots & x_{1n} \\ x_{21} & x_{22} & \cdots & x_{2n} \\ 0 & 0 & \cdots & 0 \\ \cdots & \cdots & \cdots & \cdots \\ 0 & 0 & \cdots & 0 \end{pmatrix} S,$$

或者

(9) $$R\begin{pmatrix} y_{11} & y_{12} & 0 & \cdots & 0 \\ y_{21} & y_{22} & 0 & \cdots & 0 \\ \vdots & \vdots & \vdots & & \vdots \\ y_{m1} & y_{m2} & 0 & \cdots & 0 \end{pmatrix} S,$$

其中 $R = R^{(m)}$, $S = S^{(n)}$ 均为可逆矩阵.

因此, 一个秩为 1 的极大集与一个秩为 2 的极大集, 如果它们的交集非空, 且包有此秩为 2 的极大集的特殊点, 则在变换 (1) 之下可化为下列四者之一:

秩为 1 的极大集　　秩为 2 的极大集

(i)
$$\begin{pmatrix} x_1 & x_2 & \cdots & x_n \\ 0 & 0 & \cdots & 0 \\ \cdots & \cdots & \cdots & \cdots \\ 0 & 0 & \cdots & 0 \end{pmatrix}, \quad P\begin{pmatrix} x_{11} & x_{12} & \cdots & x_{1n} \\ x_{21} & x_{22} & \cdots & x_{2n} \\ 0 & 0 & \cdots & 0 \\ \cdots & \cdots & \cdots & \cdots \\ 0 & 0 & \cdots & 0 \end{pmatrix}Q;$$

或

(ii)
$$\begin{pmatrix} y_1 & 0 & \cdots & 0 \\ y_2 & 0 & \cdots & 0 \\ \vdots & \vdots & & \vdots \\ y_m & 0 & \cdots & 0 \end{pmatrix}, \quad P\begin{pmatrix} y_{11} & y_{12} & 0 & \cdots & 0 \\ y_{21} & y_{22} & 0 & \cdots & 0 \\ \vdots & \vdots & \vdots & & \vdots \\ y_{m1} & y_{m2} & 0 & \cdots & 0 \end{pmatrix}Q;$$

或

(iii)
$$\begin{pmatrix} x_1 & x_2 & \cdots & x_n \\ 0 & 0 & \cdots & 0 \\ \cdots & \cdots & \cdots & \cdots \\ 0 & 0 & \cdots & 0 \end{pmatrix}, \quad P\begin{pmatrix} y_{11} & y_{12} & 0 & \cdots & 0 \\ y_{21} & y_{22} & 0 & \cdots & 0 \\ \vdots & \vdots & \vdots & & \vdots \\ y_{m1} & y_{m2} & 0 & \cdots & 0 \end{pmatrix}Q;$$

或

(iv)
$$\begin{pmatrix} y_1 & 0 & \cdots & 0 \\ y_2 & 0 & \cdots & 0 \\ \vdots & \vdots & & \vdots \\ y_m & 0 & \cdots & 0 \end{pmatrix}, \quad P\begin{pmatrix} x_{11} & x_{12} & \cdots & x_{1n} \\ x_{21} & x_{22} & \cdots & x_{2n} \\ 0 & 0 & \cdots & 0 \\ \cdots & \cdots & \cdots & \cdots \\ 0 & 0 & \cdots & 0 \end{pmatrix}Q.$$

在第 (i) 种情形, 可设 $Q = I$. 设 $P = (p_{ij})$, 即它们的交集由满足条件

(10)
$$\begin{pmatrix} p_{21} & p_{22} \\ p_{31} & p_{32} \\ \vdots & \vdots \\ p_{m1} & p_{m2} \end{pmatrix}\begin{pmatrix} x_{11} & x_{12} & \cdots & x_{1n} \\ x_{21} & x_{22} & \cdots & x_{2n} \end{pmatrix} = 0$$

的一切

$$P\begin{pmatrix} x_{11} & x_{12} & \cdots & x_{1n} \\ x_{21} & x_{22} & \cdots & x_{2n} \\ 0 & 0 & \cdots & 0 \\ \cdots & \cdots & \cdots & \cdots \\ 0 & 0 & \cdots & 0 \end{pmatrix}$$

组成. 令

$$\overline{P}=\begin{pmatrix} p_{21} & p_{22} \\ \vdots & \vdots \\ p_{m1} & p_{m2} \end{pmatrix}.$$

分以下两种情况讨论:

1° $\overline{P}$ 的秩为 1(当然不可能为 0). 这时, 秩为 1 的极大集包在秩为 2 的极大集之中, 交集即秩为 1 的极大集.

2° $\overline{P}$ 的秩为 2. 则仅有 $\begin{pmatrix} 0 & \cdots & 0 \\ 0 & \cdots & 0 \end{pmatrix}$ 能满足方程 (10), 因此交集即为 0.

第 (ii) 种情况与第 (i) 种情形类似讨论.

在第 (iii) 种情形, 我们施行映射

$$Z^*=ZQ^{-1},$$

即将形如 (iii) 的秩为 1 的极大集与秩为 2 的极大集仍变为形如 (iii) 的两个极大集, 但这时有 $P=I$, $Q=I$. 因此, 这时交集为

$$\begin{pmatrix} x & y & 0 & \cdots & 0 \\ 0 & 0 & 0 & \cdots & 0 \\ \cdots & \cdots & \cdots & \cdots & \cdots \\ 0 & 0 & 0 & \cdots & 0 \end{pmatrix} \quad (x,y\text{跑过}K),$$

这一个交集定义为面, 或确切地说, 秩为 1 的极大集中的面.

第 (iv) 种情形与第 (iii) 种情形类似讨论.

总结以上讨论, 我们得

定理 2 一个秩为 1 的极大集与一个秩为 2 的极大集, 如果它们的交集包有这个秩为 2 的极大集的特殊点, 则这个交集或者仅含一点 (该特殊点), 或者是秩为 1 的极大集中的面, 或者是秩为 1 的极大集本身.

由此推出

定理 3 (m,n) 长方阵仿射空间到它自身的一一映射, 如果保持粘切关系不变者, 则不仅将秩为 1 的极大集中的线映到线, 而且也将其中的面映到面.

不难写出, (m,n) 型长方阵仿射空间中面的一般方程为

$$P\begin{pmatrix} x & y & 0 & \cdots & 0 \\ 0 & 0 & 0 & \cdots & 0 \\ \cdots & \cdots & \cdots & \cdots & \cdots \\ 0 & 0 & 0 & \cdots & 0 \end{pmatrix}Q+R$$

或

$$P\begin{pmatrix} x & 0 & \cdots & 0 \\ y & 0 & \cdots & 0 \\ 0 & 0 & \cdots & 0 \\ \vdots & \vdots & & \vdots \\ 0 & 0 & \cdots & 0 \end{pmatrix}Q+R.$$

秩为 1 的极大集

$$\begin{pmatrix} x_1 & x_2 & \cdots & x_n \\ 0 & 0 & \cdots & 0 \\ \cdots & \cdots & \cdots & \cdots \\ 0 & 0 & \cdots & 0 \end{pmatrix}$$

中的面的方程为

$$\begin{pmatrix} x(q_{11},\cdots,q_{1n})+y(q_{21},\cdots,q_{2n})+(a_1,\cdots,a_n) \\ 0 \\ \vdots \\ 0 \end{pmatrix},$$

其中 x,y 独立地跑过 $K,(q_{11},\cdots,q_{1n})$ 与 $(q_{21},\cdots,q_{2n})$ 线性无关. 秩为 1 的极大集

$$\begin{pmatrix} y_1 & 0 & \cdots & 0 \\ y_2 & 0 & \cdots & 0 \\ \vdots & \vdots & & \vdots \\ y_m & 0 & \cdots & 0 \end{pmatrix}$$

中的面的方程为

$$\left(\begin{pmatrix} p_{11} \\ \vdots \\ p_{m1} \end{pmatrix}x+\begin{pmatrix} p_{12} \\ \vdots \\ p_{m2} \end{pmatrix}y+\begin{pmatrix} b_1 \\ \vdots \\ b_m \end{pmatrix}0\right),$$

其中 x,y 独立地跑过 $K,(p_{11},\cdots,p_{m1})'$ 与 $(p_{12},\cdots,p_{m2})'$ 线性无关.

§7　长方阵仿射几何的基本定理

定理 1　设 $m,n>1$, 则从 (m,n) 型长方阵仿射空间映到它自己里面的任意一一映射, 且保持粘切关系不变者, 必为下列形状:

(1) $$Z^* = PZ^{\sigma}Q + R,$$
其中 $P = P^{(m)}$ 及 $Q = Q^{(n)}$ 为可逆矩阵, R 为 $m \times n$ 矩阵, 而 σ 为体 K 之自同构. 如果 $m = n$, 则除了 (1) 之外, 还有

(2) $$Z^* = PZ^{\tau'}Q + R,$$
其中 τ 为 K 之反自同构.

【证】 我们写

$$X = \begin{pmatrix} x_1 \\ \vdots \\ x_m \end{pmatrix} = (y_1, \cdots, y_n),$$

其中

$$x_i = (x_{i1}, \cdots, x_{in}), \quad y_j = \begin{pmatrix} x_{1j} \\ \vdots \\ x_{mj} \end{pmatrix}.$$

令

$$X_i = \begin{pmatrix} 0 \\ \vdots \\ 0 \\ x_i \\ 0 \\ \vdots \\ 0 \end{pmatrix}, \quad Y_j = (0, \cdots, 0, y_j, 0, \cdots, 0).$$

设 $\mathscr{A}$ 为适合定理所给条件的一个映射. 依定理 4.1, 使 $\mathscr{A}$ 承受形如 (1) 或 (2) 的映射之后, 我们可以假设

(3) $$\mathscr{A}(X_1) = X_1^*, \quad \mathscr{A}(0) = 0.$$
依定理 6.3, 可知 $\mathscr{A}$ 诱导出将 x_1 射到 x_1^* 的一个映射, 而将线变到线, 面变到面, 所以, 依仿射几何基本定理就有

(3)′ $$x_1^* = x_1^{\alpha_1}Q_1,$$
其中 $Q_1 = Q_1^{(n)}$ 为可逆矩阵, 而 σ_1 为 K 之自同构. 使 $\mathscr{A}$ 承受形如 (1) 的映射

$$X \to [XQ_1^{-1}]^{\sigma_1^{-1}}$$

之后, 可以假定

(4) $$\mathscr{A}(X_1) = X_1,$$

对一切 X_1. 因所有的 Y_1 构成一个包有

$$0 \quad 和 \quad \begin{pmatrix} 1 & 0 & \cdots & 0 \\ 0 & 0 & \cdots & 0 \\ \cdots & \cdots & \cdots & \cdots \\ 0 & 0 & \cdots & 0 \end{pmatrix}$$

的秩为 1 的极大集, 故依定理 4.2 有

(5) $$\mathscr{A}(Y_1) = Y_1^*,$$

而依仿射几何基本定理可设

(5)′ $$y_1^* = P_1 y_1^{\tau_1},$$

其中 $P_1 = P_1^{(m)}$ 为可逆矩阵, τ_1 为 K 之自同构. 将

$$\begin{pmatrix} x_{11} & 0 & \cdots & 0 \\ 0 & 0 & \cdots & 0 \\ \cdots & \cdots & \cdots & \cdots \\ 0 & 0 & \cdots & 0 \end{pmatrix} \quad (x_{11} \in K)$$

代入 (4) 和 (5)′ 并比较之, 得

(6) $$\begin{pmatrix} x_{11} \\ 0 \\ \vdots \\ 0 \end{pmatrix} = P_1 \begin{pmatrix} x_{11} \\ 0 \\ \vdots \\ 0 \end{pmatrix}^{\tau_1}.$$

令 $P_1 = (p_{ij})_{1 \leqslant i,j \leqslant m}$. 在 (6) 中取 $x_{11} = 1$ 得

$$p_{11} = 1, \quad p_{21} = p_{31} = \cdots = p_{m1} = 0.$$

由此及 (6) 推出 $x_{11} = x_{11}^{\tau_1}$ 对一切 $x_{11} \in K$, 即 τ_1 为 K 之单位自同构,$\tau_1 = 1$. 那么, 使 $\mathscr{A}$ 承受形如 (1) 的映射

$$X \to P_1^{-1} X$$

之后, 除了仍旧有 (4) 之外, 还有

$$\mathscr{A}(Y_1) = Y_1,$$

对一切 Y_1.

注意到所有的 X_i 组成一个包有

$$0 \quad 和 \quad \begin{pmatrix} 0 & 0 & \cdots & 0 \\ \cdots & \cdots & \cdots & \cdots \\ 0 & 0 & \cdots & 0 \\ 1 & 0 & \cdots & 0 \\ 0 & 0 & \cdots & 0 \\ \cdots & \cdots & \cdots & \cdots \\ 0 & 0 & \cdots & 0 \end{pmatrix} \quad (第i行)$$

的秩为 1 的极大集, 因此依定理 4.2 有

(7) $$\mathscr{A}(X_i) = X_i^* \quad (i = 2, \cdots, m).$$

再依仿射几何基本定理有

(7)′ $$x_i^* = x_i^{\sigma_i} Q_i \quad (i = 2, \cdots, m),$$

其中 σ_i 为 K 之自同构, $Q_i = Q_i^{(n)}$ 为可逆矩阵. 包有

$$0 \quad 和 \quad \begin{pmatrix} 0 & \cdots & 0 & 1 & 0 & \cdots & 0 \\ 0 & \cdots & 0 & 0 & 0 & \cdots & 0 \\ \vdots & & \vdots & \vdots & \vdots & & \vdots \\ 0 & \cdots & 0 & 0 & 0 & \cdots & 0 \end{pmatrix}$$

(第j列)

的秩为 1 的极大集而不等于 X_1 的必是 Y_j, 所以

(8) $$\mathscr{A}(Y_j) = Y_j^* \quad (j = 2, \cdots, n).$$

依仿射几何基本定理有

(8)′ $$y_j^* = P_j y_j^{\tau_j},$$

其中 τ_j 为 K 之自同构, $P_j = P_j^{(m)}$ 为可逆矩阵.

以 $x_{ij}E_{ij}$ 表 X_i 与 Y_j 的交集中的一个元素, 则

$$\mathscr{A}(x_{ij}E_{ij}) = x_{ij}^* E_{ij}.$$

因此 Q_i 和 P_j 都是对角形矩阵, 记作

$$Q_i = [q_{i1}, \cdots, q_{in}], \quad P_j = [p_{1j}, \cdots, p_{mj}].$$

比较 (7)′ 和 (8)′ 即得

(9) $$x_{ij}^{\sigma_i} q_{ij} = p_{ij} x_{ij}^{\tau_j}.$$

上式对于 K 中所有 x_{ij} 都成立. 特别, 如 $x_{ij} = 1$, 我们就有 $q_{ij} = p_{ij}$. 因此, 当 $i = 1$ 时, $p_{1j} = 1$ 而 $\tau_j = 1$, 对所有 $j = 1, \cdots, m$. 于是 σ_i 都是内自同构. 前已说

过, $P_1 = I^{(m)}$, 于是由 (9), 令 $j=1$ 可推出 $q_{i1}=1$ 及 $\sigma_i = 1$, 对 $i=1,\cdots,n$. 再者, 由 x_1 及 x_i 的线性相关性推出 $x_1 = x_1Q_1$ 及 x_iQ_i 线性相关, 于是 $Q_i = q_iI^{(n)}$. 因 $Q_i = [1, q_{i2}, \cdots, q_{in}]$, 故 $Q_i = I^{(n)}$, 对于所有 i. 同样, $P_j = I^{(m)}$, 对所有 j, 于是我们有

$$\mathscr{A}(X_i) = X_i, \quad \mathscr{A}(Y_j) = Y_j.$$

现在我们来证 $\mathscr{A}(X) = X$, 对一切 X. 分别讨论 $m \leqslant n$ 及 $m \geqslant n$ 两种情形. 因为它们可相似地加以讨论, 所以我们只讨论 $m \leqslant n$ 这个情形.

令

$$\mathscr{A}\begin{pmatrix} x_1 \\ x_2 \\ \vdots \\ x_m \end{pmatrix} = \begin{pmatrix} x_1^* \\ x_2^* \\ \vdots \\ x_m^* \end{pmatrix}.$$

设 $\begin{pmatrix} x_1 \\ x_2 \\ \vdots \\ x_m \end{pmatrix}$ 之秩为 m, 则 $\begin{pmatrix} x_1^* \\ x_2^* \\ \vdots \\ x_m^* \end{pmatrix}$ 之秩也为 m. 因为

$$\mathscr{A}\begin{pmatrix} x_1 - \lambda_2 x_2 - \cdots - \lambda_m x_m \\ 0 \\ \vdots \\ 0 \end{pmatrix} = \begin{pmatrix} x_1 - \lambda_2 x_2 - \cdots - \lambda_m x_m \\ 0 \\ \vdots \\ 0 \end{pmatrix},$$

所以

$$\begin{pmatrix} x_1^* - x_1 + \lambda_2 x_2 + \cdots + \lambda_m x_m \\ x_2^* \\ \vdots \\ x_m^* \end{pmatrix}$$

的秩等于 $m-1$, 对于所有 $\lambda_2, \cdots, \lambda_m \in K$. 因此

$$x_1 = x_1^* + \sum_{j=2}^{m} \mu_j x_j^*,$$

$$x_k = \sum_{j=2}^{m} \mu_{kj} x_j^* \quad (2 \leqslant k \leqslant m).$$

将同样方法应用于第 i 行, 就有

$$x_i = x_i^* + \sum_{j \neq i} v_j^{(i)} x_j^*,$$

$$x_k = \sum_{j \neq i} v_{kj}^{(i)} x_j^* \quad (k \neq i).$$

消去 x_1 就有

$$x_1^* = \sum_{j \neq i} v_{1j}^{(i)} x_j^* - \sum_{j=2}^{m} \mu_j x_j^*.$$

因为 $x_1^*, \cdots, x_m^*$ 线性无关, 所以

$$\mu_i = 0 \quad (2 \leqslant i \leqslant m).$$

因此 $x_1 = x_1^*$. 同样, 我们有 $x_i = x_i^*$, 即如果 X 之秩为 m, 则有

$$\mathscr{A}(X) = X. \tag{10}$$

现在假定 X 之秩 $< m$. 我们分以下两个情形来研究.

(i)K 中元素个数多于 2 的情形. 如果 $x_{11} \neq 0$, 则由 (10) 知

$$\mathscr{A}\begin{pmatrix} x_{11} & x_{12} & \cdots & x_{1m} & x_{1,m+1} & \cdots & x_{1n} \\ 0 & \lambda_2 & & 0 & 0 & \cdots & 0 \\ \vdots & & \ddots & \vdots & \vdots & & \vdots \\ 0 & \cdots & & \lambda_m & 0 & \cdots & 0 \end{pmatrix}$$

$$= \begin{pmatrix} x_{11} & x_{12} & \cdots & x_{1m} & x_{1,m+1} & \cdots & x_{1n} \\ 0 & \lambda_2 & & 0 & 0 & \cdots & 0 \\ \vdots & & \ddots & \vdots & \vdots & & \vdots \\ 0 & \cdots & & \lambda_m & 0 & \cdots & 0 \end{pmatrix},$$

对于任意 $\lambda_2, \cdots, \lambda_m \neq 0$. 于是

$$\begin{pmatrix} x_{11}^* - x_{11} & x_{12}^* - x_{12} & \cdots & x_{1m}^* - x_{1m} & x_{1m+1}^* - x_{1m+1} & \cdots & x_{1n}^* - x_{1n} \\ x_{21}^* & x_{22}^* - \lambda_2 & & x_{2m}^* & x_{2m+1}^* & \cdots & x_{2n}^* \\ \vdots & & \ddots & \vdots & \vdots & & \vdots \\ x_{m1}^* & x_{m2}^* & \cdots & x_{mm}^* - \lambda_m & x_{mm+1}^* & \cdots & x_{mn}^* \end{pmatrix}$$

的秩 $< m$, 对任意 $\lambda_2, \cdots, \lambda_3 \neq 0$. 于是仅可能

$$x_{11}^* - x_{11} = 0.$$

如果 $x_{11}^* \neq 0$, 我们考虑 $\mathscr{A}^{-1}$, 因而证得 $x_{11}^* = x_{11}$. 同样可以证明 $x_{ij}^* = x_{ij}$. 因此在这情形定理得证.

(ii)K 只有两个元素的情形. 先考虑 $m=n=2$ 的情形. 这时我们有

$$\mathscr{A}(X_i)=X_i,\quad \mathscr{A}(Y_i)=Y_i\quad (i=1,2),$$
$$\mathscr{A}(X)=X, \text{如}X\text{的秩为}2.$$

秩为 1 的矩阵中, 除属于 $X_i, Y_i(i=1,2)$ 的以外, 只有 $\begin{pmatrix}1&1\\1&1\end{pmatrix}$, 因此必有

$$\mathscr{A}\begin{pmatrix}1&1\\1&1\end{pmatrix}=\begin{pmatrix}1&1\\1&1\end{pmatrix}.$$

这样,

$$\mathscr{A}(X)=X$$

对一切 2×2 矩阵 X. 因此定理得证.

再研究 $n\geqslant 3$ 的情形. 设

$$X=\begin{pmatrix}x_1\\x_2\\\vdots\\x_m\end{pmatrix}$$

的秩为 $m-1$, 于是行向量 $x_1,x_2,\cdots,x_m$ 中必有 $m-1$ 个线性无关, 不妨设 $x_2,\cdots,x_m$ 线性无关. 我们选择 $\lambda_1,\cdots,\lambda_n\in K$. 使矩阵

$$\widetilde{X}=\begin{pmatrix}\lambda_1 & \cdots & \lambda_n\\ & x_2 & \\ & \vdots & \\ & x_m & \end{pmatrix}$$

的秩为 m. 于是由 (i) 有

$$\mathscr{A}(\widetilde{X})=\widetilde{X}.$$

设

$$\mathscr{A}(X)=\begin{pmatrix}x_1^*\\x_2^*\\\vdots\\x_m^*\end{pmatrix}=\begin{pmatrix}x_{11}^* & x_{12}^* & \cdots & x_{1n}^*\\ & x_2^* & & \\ & \vdots & & \\ & x_m^* & & \end{pmatrix}.$$

由于 $\widetilde{X}$ 与 X 粘切, 所以

$$\begin{pmatrix} x_{11}^*-\lambda_1 & x_{12}^*-\lambda_2 & \cdots & x_{1n}^*-\lambda_n \\ & x_2^*-x_2 & & \\ & \vdots & & \\ & x_m^*-x_m & & \end{pmatrix}$$

的秩也为 1. 由于 $n \geqslant 3$, 故使 $\widetilde{X}$ 的秩为 m 的 $\lambda_1, \cdots, \lambda_n$ 中有 $n-1 \geqslant 2$ 个可任意选取, 所以必须

$$x_i^*-x_i=0 \quad (i=2, \cdots, m).$$

这样就有

$$\mathscr{A}(X)=\begin{pmatrix} x_1^* \\ x_2 \\ \vdots \\ x_m \end{pmatrix}.$$

如果 $x_1 \neq (0, \cdots, 0)$, 则有 $x_1, x_{i_2}, \cdots, x_{i_{m-1}}$ 线性无关, 于是可推得 $x_1^*=x_1$. 如果 $x_1=(0, \cdots, 0)$, 这时必有 $x_1^*=(0, \cdots, 0)$. 因为否则对 $\mathscr{A}(X)$ 施行逆映射 $\mathscr{A}^{-1}$, 则会有 $x_1=x_1^* \neq (0, \cdots, 0)$, 因而发生矛盾. 于是有

$$\mathscr{A}(X)=X, \text{对一切秩为} m-1 \text{的} X.$$

设 X 的秩为 $m-2$. 不妨设 $x_3, \cdots, x_m$ 线性无关. 今选取 $\lambda_1, \cdots, \lambda_n$, 使

$$\widetilde{X}=\begin{pmatrix} \lambda_1 & \cdots & \lambda_n \\ & x_2 & \\ & x_3 & \\ & \vdots & \\ & x_m & \end{pmatrix}$$

的秩为 $m-1$. 于是由刚才的结论有

$$\mathscr{A}(\widetilde{X})=\widetilde{X}.$$

由于 $(\widetilde{X}-X)$ 的秩为 1, 故

$$\begin{pmatrix} x_{11}^*-\lambda_1 & \cdots & x_{1n}^*-\lambda_n \\ & x_2^*-x_2 & \\ & \vdots & \\ & x_m^*-x_m & \end{pmatrix}$$

的秩也为 1. 于是同样有 $x_i^* = x_i (i = 1, \cdots, m)$. 即

$$\mathscr{A}(X) = X, \text{对一切秩为} m-2 \text{的} X.$$

这种步骤显然可用数学归纳法推证下去, 因而得到

$$\mathscr{A}(X) = X, \text{对一切} m \times m \text{矩阵} X.$$

于是基本定理得证.

没有什么太大的困难可以将我们的定理推广成下面的形状: 令 $K_{m,n}(m, n \geqslant 1)$ 为 K 上所有 $m \times n$ 矩阵之全体, $K'_{m',n'}(m', n' \geqslant 1)$ 为 K' 上所有 $m' \times n'$ 矩阵之全体. 如果有一个一对一的映射将 $K_{m,n}$ 变到 $K'_{m',n'}$ 之上而保持粘切关系不变, 则有 $m = m'$, $n = n'$ 或 $m = n'$, $n = m'$. 在第一种情形, K 和 K' 同构, 如果视为同一, 则得 §1 变换 (4). 在第二种情形, K 和 K' 反同构, 而映射可写成

$$Z^* = P Z^{\tau'} Q + R,$$

其中 τ 表反同构.

§8 长方阵射影几何的基本定理

基于长方阵仿射几何的基本定理可推出下述长方阵射影几何的基本定理

定理 1 将 $(m, m+n)$ 型长方阵射影空间映到它自身之上的任意 1-1 映射且保持粘切关系者必为 §1 形状 (1). 如果 $m = n$, 则还有另一种形状的变换即 §2 所描写的.

证明由读者自行补出.

第六章　线性群的构造及自同构

§1　复　　习

我们回忆一下以前几章所研究过的线性群. 如像以前一样, 以 K 表体.

K 上 n 级一般线性群 $GL_n(K)$ 是 K 中所有 n 行可逆矩阵对乘法而言所组成的群.

$GL_n(K)$ 的子群 $SL_n(K)$ 为由所有元素 $T_{ij}(\lambda)(1 \leqslant i; j \leqslant n; i \neq j; \lambda \in K^*)$ 所生成者, 称为 n 级特殊线性群. $T_{ij}(\lambda)$ 为将 n 级单位矩阵中 (i,j) 位置的元素易之以 λ 所得到的矩阵.

在第三章中曾证明 $GL_n(K)/SL_n(K)$ 为 Abel 群, 而且与 K 的乘法群 K^* 对 K^* 的换位子群的商群同构. 在第三章中亦曾证明 $SL_n(K)$ 是 $GL_n(K)$ 的换位子群, 除非 $n=2$ 而 K 只有两个元素.

$GL_n(K)$ 的中心由形如 λI 的矩阵所组成, 而 λ 跑过 K 中所有非零中心元素. $GL_n(K)$ 对它中心的商群称为 K 上 n 级射影一般线性群: $PGL_n(K)$.

$SL_n(K)$ 对其中心的射影群称为 K 上 n 级射影特殊线性群, 记作 $PSL_n(K)$. 可以证明, $SL_n(K)$ 的中心由形如 λI 的元素所组成, 而 λ 属于 K 之中心, $\lambda \neq 0, \lambda^n$ 属于 K^* 之换位子群 C.

如果 K 为 p^l 个元素的域, 则指数 $GL_n(K):SL_n(K)$ 以及 $SL_n(K)$ 的中心的阶分别为 p^l-1 及 (n, p^l-1). 再者, $GL_n(K)/SL_n(K)$ 和 $SL_n(K)$ 的中心都是循环群.

§2　在 $SL_n(K)$ 之下矩阵的相似

为要研究线性群的构造及自同构, 有时得研究矩阵在 $SL_n(K)$ 之下的相似.

定义 1　n 行矩阵 A 和 B 称为在 $SL_n(K)$ 之下相似, 如有矩阵 $Q \in SL_n(K)$ 存在, 使得

(1)
$$A = Q^{-1}BQ.$$

亦称 A 在 $SL_n(K)$ 之下相似于 B.

显然, 在 $SL_n(K)$ 之下矩阵的相似关系是一个等价关系. 再者, 我们有

定理 1　任意 n 行矩阵, 如其秩为 r, 则在 $SL_n(K)$ 之下相似于下列形状的一

个矩阵:

$$\begin{pmatrix} u_1 \\ u_2 \\ \vdots \\ u_r \\ 0 \\ \vdots \\ 0 \end{pmatrix},$$

其中 $u_1, u_2, \cdots, u_r$ 为 r 个线性无关的行.

【证】 设 A 为 n 行矩阵且秩为 r, 则有一置换矩阵 P 存在, 使得 $P^{-1}AP$ 的前 r 行线性无关, 可是 $\det(P) = 1$ 或 -1. 如 $\det(P) = -1 \neq 1$, 则矩阵 $[1, \cdots, 1, -1]P$ 属于 $SL_n(K)$, 而

$$\{[1, \cdots, 1, -1]P\}^{-1}A\{[1, \cdots, 1, -1]P\}$$

的前 r 行亦线性无关, 因此不妨假设 $P \in SL_n(K)$. 写

$$P^{-1}AP = \begin{pmatrix} u_1 \\ u_2 \\ \vdots \\ u_n \end{pmatrix},$$

而

$$u_i = \sum_{j=1}^{r} b_{ij}u_j \quad (r+1 \leqslant i \leqslant n).$$

令 $B = B^{(n-r,r)} = (b_{ij})$, 则

$$\begin{pmatrix} u_1 \\ u_2 \\ \vdots \\ u_n \end{pmatrix} = \begin{pmatrix} I^{(r)} & 0 \\ B & I^{(n-r)} \end{pmatrix} \begin{pmatrix} u_1 \\ \vdots \\ u_r \\ 0 \\ \vdots \\ 0 \end{pmatrix}.$$

因此令

$$Q = P\begin{pmatrix} I & 0 \\ B & I \end{pmatrix},$$

则

$$Q^{-1}AQ=\begin{pmatrix} u_1 \\ \vdots \\ u_r \\ 0 \\ \vdots \\ 0 \end{pmatrix}.$$

定理证毕.

我们更进一步讨论幂等矩阵在 $SL_n(K)$ 之下的相似问题.

定理 2 r 秩的幂等矩阵在 $SL_n(K)$ 之下相似于

(2) $$[1,\cdots,1,0,\cdots,0],$$

其中 1 的个数为 r.

【证】 设 A 为 r 秩的幂等矩阵. 依定理 1, 不妨设

$$A=\begin{pmatrix} A_1 & A_2 \\ 0 & 0 \end{pmatrix},$$

其中 $A_1=A_1^{(r)}$ 而 $A_2=A_2^{(r,n-r)}$. 由 $A^2=A$ 推出

$$A_1^2=A_1,\quad A_1\cdot A_2=A_2,$$

因此 A_1 的秩为 r, 即 A_1 为可逆矩阵, 于是由 $A_1^2=A_1$ 推出 $A_1=I$. 令

$$P=\begin{pmatrix} I^{(r)} & A_2 \\ 0 & I^{(n-r)} \end{pmatrix},$$

则 $P\in SL_n(K)$, 而

$$PAP^{-1}=[1,\cdots,1,0,\cdots,0],$$

其中 1 的个数为 r. 定理证毕.

关于 $GL_n(K)$ 中元素在 $SL_n(K)$ 之下相似的问题我们不准备作一般性的讨论. 在本节中, 我们只准备讨论 $GL_n(K)$ 中元素 A, 而 $A-I$ 的秩为 1 者, 在 $SL_n(K)$ 之下的相似问题. 我们区别 $A-I$ 不是幂零矩阵及是幂零矩阵这两种情形. 当 $A-I$ 不是幂零矩阵时, 我们将 A 称为 $GL_n(K)$ 中的 D- 矩阵, 而当 $A-I$ 是幂零矩阵时, 我们将 A 称为 $GL_n(K)$ 中的平延.

定理 3 设 A 为 $GL_n(K)$ 中之 D- 矩阵, 则 A 在 $SL_n(K)$ 之下相似于形如 $[1,\cdots,1,\mu]$ 的矩阵.

【证】 依定理 1, 不妨设

$$A-I=\begin{pmatrix}\mu & v\\ 0 & 0\end{pmatrix},$$

其中 $\mu\in K$ 而 v 为 $n-1$ 维向量, 因 $A-I$ 非幂零, 故 $\mu\neq 0$. 令

$$P=\begin{pmatrix}1 & \mu^{-1}v\\ 0 & I^{(n-1)}\end{pmatrix},$$

则 $P\in SL_n(K)$, 而

$$P(A-I)P^{-1}=\begin{pmatrix}\mu & 0\\ 0 & 0\end{pmatrix}.$$

再令

$$Q=\begin{pmatrix}0 & & 1\\ & I & \\ -1 & & 0\end{pmatrix},$$

则 $Q\in SL_n(K)$, 而

$$QP(A-I)P^{-1}Q^{-1}=[0,\cdots,0,\mu].$$

因之

$$(QP)A(QP)^{-1}=[1,\cdots,1,\mu']\quad(\mu'=1+\mu).$$

定理 4 设 A 为 $GL_n(K)$ 中之平延, 则 A 在 $GL_n(K)$ 之下相似于形如

$$\begin{pmatrix}1 & 1 & 0 & \cdots & 0\\ 0 & 1 & 0 & \cdots & 0\\ 0 & 0 & 1 & \cdots & 0\\ \vdots & \vdots & \vdots & \ddots & \vdots\\ 0 & 0 & 0 & \cdots & 1\end{pmatrix}\tag{3}$$

的矩阵. 因之 $GL_n(K)$ 中之平延皆属于 $SL_n(K)$.

【证】 依定理 1, 不妨设

$$A-I=\begin{pmatrix}\mu & v\\ 0 & 0\end{pmatrix},$$

其中 $\mu\in K$ 而 v 为 $n-1$ 维向量. 因 $A-I$ 幂零, 故 $\mu=0$; 因之 $v\neq 0$, 于是依第三章定理 4.4, 有 $n-1$ 行可逆矩阵 $\begin{pmatrix}v\\ Q\end{pmatrix}$ 存在, 其中 $Q=Q^{(n-2,n-1)}$. 于是

$$v\begin{pmatrix}v\\ Q\end{pmatrix}^{-1}=(1,0,\cdots,0).$$

令

$$P = \begin{pmatrix} 1 & 0 \\ 0 & \begin{pmatrix} v \\ Q \end{pmatrix}^{-1} \end{pmatrix},$$

则 $P \in GL_n(K)$, 而

$$P^{-1}(A-I)P = \begin{pmatrix} 0 & 1 & 0 & \cdots & 0 \\ 0 & 0 & 0 & \cdots & 0 \\ \cdots & \cdots & \cdots & \cdots & \cdots \\ 0 & 0 & 0 & \cdots & 0 \end{pmatrix}.$$

因之

$$P^{-1}AP = \begin{pmatrix} 1 & 1 & 0 & \cdots & 0 \\ 0 & 1 & 0 & \cdots & 0 \\ 0 & 0 & 1 & \cdots & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & 0 & \cdots & 1 \end{pmatrix}.$$

易见 (3)$\in SL_n(K)$. 因 $SL_n(K)$ 为 $GL_n(K)$ 的正规子群, 故 $A \in SL_n(K)$.

定理 5 设 $n \geqslant 3$, 则 $GL_n(K)$ 中平延皆在 $SL_n(K)$ 之下相似于形如 (3) 的矩阵; 而 $GL_2(K)$ 中之平延在 $SL_2(K)$ 之下皆相似于形如 $\begin{pmatrix} 1 & \mu \\ 0 & 1 \end{pmatrix}$ 的矩阵, $\mu \in K^*$.

【证】 设 A 为 $GL_n(K)$ 中之平延. 依定理 4, 有 $P \in GL_n(K)$ 存在, 使

$$P^{-1}AP = \begin{pmatrix} 1 & 1 & 0 & \cdots & 0 \\ 0 & 1 & 0 & \cdots & 0 \\ 0 & 0 & 1 & \cdots & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & 0 & \cdots & 1 \end{pmatrix}.$$

依第三章定理 8.1, 可将 P 写作

$$P = BD(\mu),$$

其中 $B \in SL_n(K)$ 而 $D(\mu) = [1, \cdots, 1, \mu]$. 因此当 $n \geqslant 3$ 时, 我们有

$$B^{-1}AB = \begin{pmatrix} 1 & 1 & 0 & \cdots & 0 \\ 0 & 1 & 0 & \cdots & 0 \\ 0 & 0 & 1 & \cdots & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & 0 & \cdots & 1 \end{pmatrix},$$

而当 $n = 2$ 时, 我们有

$$B^{-1}AB = \begin{pmatrix} 1 & \mu^{-1} \\ 0 & 1 \end{pmatrix}.$$

自然会发生这样的问题, 即 $SL_2(K)$ 中任意两个平延是否在 $SL_2(K)$ 之下相似? 一般说来, 并不如此. 例如, 设 K 为实数域, 则

$$\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} \quad 和 \quad \begin{pmatrix} 1 & -1 \\ 0 & 1 \end{pmatrix}$$

在 $SL_2(K)$ 之下不相似. 实际上, 由

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix}\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} 1 & -1 \\ 0 & 1 \end{pmatrix}\begin{pmatrix} a & b \\ c & d \end{pmatrix}$$

推出 $c = 0$ 及 $a = -d$. 因之 $\begin{pmatrix} a & b \\ c & d \end{pmatrix}$ 的行列式为 $-a^2$, 而 $-a^2$ 决不能等于 1.

§3　$PSL_n(K)$ 的单性

在第二章 §5 中曾证明, 除开 K 只有 2 元或 3 元之外, $PSL_2(K)$ 永为单群. 本节将证明 $PSL_n(K)$ 为单群, 对任意 K 及 $n \geqslant 3$. 在证明这个结果之前, 我们先注意次之事实.

定理 1　设 $n \geqslant 2$, 则 $SL_n(K)$ 由 $GL_n(K)$ 中所有平延所生成.

【证】　我们知道 $SL_n(K)$ 由一切 $T_{ij}(\lambda)(1 \leqslant i, j \leqslant n; i \neq j; \lambda \in K^*)$ 所生成, 而 $T_{ij}(\lambda)$ 皆平延. 另一方面, 依定理 2.5, $SL_n(K)$ 包有 $GL_n(K)$ 中所有平延, 因此 $SL_n(K)$ 由 $GL_n(K)$ 中所有平延所组成.

引理　设 $n \geqslant 2$, 而 $\mathfrak{N}$ 是 $GL_n(K)$ 的一个子群, 并且假定它在 $SL_n(K)$ 之下不变. 如果 $\mathfrak{N}$ 包有一个平延, 则 $\mathfrak{N} \supseteq SL_n(K)$.

【证】　$n = 2$ 的情形在第二章 §5 中已经证明. 至于当 $n \geqslant 3$ 时, 依定理 2.5, $GL_n(K)$ 中平延在 $SL_n(K)$ 之下皆相似, 因之如 $\mathfrak{N}$ 包有一个平延, 它就包有所有平延, 于是 $\mathfrak{N} \supseteq SL_n(K)$.

定理 2 设 $n \geqslant 2$ 而 $\mathfrak{N}$ 为 $GL_n(K)$ 的子群, 并假定它在 $SL_n(K)$ 之下不变. 于是或者 $\mathfrak{N}$ 是 $GL_n(K)$ 的中心的一个子群, 或者 $\mathfrak{N} \supseteq SL_n(K)$, 除非 $n = 2$ 而 $K = F_2$ 或 F_3.

【证】 $n = 2$ 的情形在第二章 §5 中已经证明, 现在设 $n \geqslant 3$. 设 $\mathfrak{N}$ 不是 $GL_n(K)$ 的中心的一个子群, 则 $\mathfrak{N}$ 含一元素 A, 而 A 不在 $GL_n(K)$ 的中心之中. 于是有一 $B = T_{ij}(\lambda)$ 存在, 使 $AB \neq BA$. 考虑 $T = B^{-1}A^{-1}BA$. 因 $\mathfrak{N}$ 在 $SL_n(K)$ 之下不变, 故 $T \in \mathfrak{N}$. 写 $B = I + E$, 而 $E^2 = 0$, 同时 E 的秩为 1, 于是 $B^{-1} = I - E$, 而

$$T = (I - E)A^{-1}(I + E)A = I + A^{-1}EA - EA^{-1}(I + E)A.$$

写 $S = A^{-1}EA - EA^{-1}(I + E)A$, 则 $T = I + S, S \neq 0$. 因为 $A^{-1}EA$ 的秩为 1, 而 $EA^{-1}(I + E)A$ 的秩顶多是 1, 故 S 的秩 $\leqslant 2$.

依定理 2.1, 有 $P \in SL_n(K)$, 使得

$$PSP^{-1} = \begin{pmatrix} U^{(2,n)} \\ 0^{(n-2,n)} \end{pmatrix}.$$

于是元素

$$T_1 = PTP^{-1} = \begin{pmatrix} A_1^{(2)} & B_1 \\ 0 & I^{(n-2)} \end{pmatrix}$$

就包在 $\mathfrak{N}$ 中. 再者, 我们可以假定 $\mathfrak{N}$ 包有形如

$$D = \begin{pmatrix} I^{(2)} & N^{(2,n-2)} \\ 0 & I^{(n-2)} \end{pmatrix} \quad (N \neq 0)$$

的一个元素. 因为如果 $A_1^{(2)} = I^{(2)}$, 则 T_1 就是这样一个元素; 而如 $A_1^{(2)} \neq I^{(2)}$, 则因

$$\begin{pmatrix} A_1 & B_1 \\ 0 & I \end{pmatrix}\begin{pmatrix} I & X \\ 0 & I \end{pmatrix}\begin{pmatrix} A_1 & B_1 \\ 0 & I \end{pmatrix}^{-1}\begin{pmatrix} I & X \\ 0 & I \end{pmatrix}^{-1} = \begin{pmatrix} I & (A_1 - I)X \\ 0 & I \end{pmatrix},$$

我们可以选取 X 使得 $(A_1 - I)X \neq 0$, 因而得到一个形如 D 的元素. 注意 N 之秩为 1 或 2. 如 N 的秩为 1, 则 D 即为一平延, 于是依引理我们有 $\mathfrak{N} \supseteq SL_n(K)$. 以下研究 N 的秩为 2 的情形. 由于

$$\begin{pmatrix} Q_1 & 0 \\ 0 & Q_2 \end{pmatrix}\begin{pmatrix} I & N \\ 0 & I \end{pmatrix}\begin{pmatrix} Q_1^{-1} & 0 \\ 0 & Q_2^{-1} \end{pmatrix} = \begin{pmatrix} I & Q_1NQ_2^{-1} \\ 0 & I \end{pmatrix},$$

所以依第三章定理 5.3, 我们可以选取 $Q_1 \in GL_2(K)$ 及 $Q_2 \in GL_{n-2}(K)$, 使得 $Q_1NQ_2^{-1} = \begin{pmatrix} 1 & 0 & 0 & \cdots & 0 \\ 0 & 1 & 0 & \cdots & 0 \end{pmatrix}$. 因之, 我们可以选取 $Q_1 \in SL_2(K)$ 及 $Q_2 \in SL_{n-2}(K)$, 使得

$$Q_1NQ_2^{-1} = \begin{pmatrix} 1 & 0 & 0 & \cdots & 0 \\ 0 & \lambda & 0 & \cdots & 0 \end{pmatrix} \quad (\lambda \neq 0).$$

于是

$$\begin{pmatrix} 1 & -1 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix}\begin{pmatrix} 1 & 0 & 1 & 0 \\ 0 & 1 & 0 & \lambda \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix}\begin{pmatrix} 1 & -1 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix}^{-1}\begin{pmatrix} 1 & 0 & 1 & 0 \\ 0 & 1 & 0 & \lambda \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix}^{-1}$$
$$= \begin{pmatrix} 1 & 0 & 0 & -\lambda \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix}$$

为一 $T_{ij}(\lambda)$, 本定理仍从上面引理推出.

适才证明的定理有下面一些特殊情形及推论.

定理 3　设 $n \geqslant 2$, 则除非 $n = 2$ 及 $K = F_2$ 或 $F_3, GL_n(K)$ 的任何正规子群, 如不含在中心之中, 必包含 $SL_n(K)$.

定理 4　设 $n \geqslant 2$, 则除非 $n = 2$ 及 $K = F_2$ 或 $F_3, SL_n(K)$ 的任何正规子群, 如不含在它的中心之中, 就与 $SL_n(K)$ 相重.

定理 5　设 $n \geqslant 2$, 则除非 $n = 2$ 及 $K = F_2$ 或 $F_3, PSL_n(K)$ 皆单群.

定理 6　设 $n \geqslant 2$, 则除非 $n = 2$ 及 $K = F_2$ 或 $F_3, SL_n(K)$ 是它自己的换位子群.

【证】　注意 $SL_n(K)$ 的换位子群含有一个非中心元素:

$$\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}\begin{pmatrix} 1 & 0 \\ -1 & 1 \end{pmatrix}\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}^{-1}\begin{pmatrix} 1 & 0 \\ -1 & 1 \end{pmatrix}^{-1} = \begin{pmatrix} 1 & 1 \\ 1 & 2 \end{pmatrix},$$

由此即可推出本定理.

最后, 我们研究 K 为有限域且含 $q = p^l$ 个元素的情形. 这时 $PSL_n(K)$ 的阶为

$$\Phi = \frac{1}{d(q-1)}(q^n - 1)(q^n - q)\cdots(q^n - q^{n-1}),$$

其中 $d=(n,q-1)$. 因此除了交错群 $\mathfrak{A}_n(n\neq 4)$ 之外, 我们又得到了一系列有限单群 $PSL_n(K)$.

$GL_n(K)$ 有正规群列

$$GL_n(K)\supset SL_n(K)\supset Z_n\cap SL_n(K)\supset\{I\},$$

其中 Z_n 为 $GL_n(K)$ 的中心. 根据定理 5, 除了 $n=2$ 及 $K=F_2$ 或 F_3 这两个情形以外, 这个正规群列只可能在 $GL_n(K)$ 及 $SL_n(K)$ 之间与 $Z_n\cap SL_n(K)$ 及 $\{I\}$之间精致化. 令

$$p^l-1=p_1p_2\cdots p_m \quad 及 \quad d=q_1q_2\cdots q_k,$$

p^l-1 为 $GL_n(K)/SL_n(K)$ 之阶, 而 d 为 $Z_n\cap SL_n(K)$ 之阶, 则 $GL_n(K)$ 的组合因子是

$$p_1,p_2,\cdots,p_m,\varPhi,q_1,q_2,\cdots,q_k.$$

当 $n=2$ 而 K 只有 2 元时, $GL_2(K)=SL_2(K)=\mathfrak{S}_3$, 这时 $GL_2(K)$ 的组合因子是 2 和 3.

当 $n=2$ 而 K 只含 3 元时, $GL_2(K)$ 的组合因子是 2, 3, 2, 2, 2. 这时 $GL_2(K)$ 有生成元

$$A=\begin{pmatrix}-1&0\\1&1\end{pmatrix},\quad B=\begin{pmatrix}0&1\\-1&1\end{pmatrix},\quad C=\begin{pmatrix}0&-1\\1&0\end{pmatrix},$$

$$D=\begin{pmatrix}1&-1\\1&-1\end{pmatrix},\quad E=\begin{pmatrix}-1&0\\0&-1\end{pmatrix},$$

而这些元素之中, A 的行列式为 -1, 而其余元素的行列式皆为 1. 我们有以下关系:

$$\begin{aligned}
&E^2=I\\
&D^2=E,\quad DE=ED,\\
&C^2=E,\quad CE=EC,\quad CD=EDC,\\
&B^3=E,\quad BE=EB,\quad BD=EDBC,\quad BC=ECDB,\\
&A^2=I,\quad AE=EA,\quad AD=CA,\quad AC=DA,\\
&\qquad\quad AB=ECB^2AC
\end{aligned}$$

因之 $GL_2(K)$ 有组合群列

$$\begin{aligned}GL_2(K)=\{E,D,C,B,A\}\supset SL_2(K)&=\{E,D,C,B\}\\ \supset\{E,D,C\}\supset\{E,D\}&\supset Z\supset\{I\},\end{aligned}$$

而这些群的阶分别是 48, 24, 8, 4, 2.

显然, 在这两个情形, $PSL_2(K)$ 不是单群.

§4 对　　合

在本章之其余部分我们要研究阶数为 $n \geqslant 3$ 的线性群的自同构.

定义 1　非中心元素 $A \in GL_n(K)$ 称为对合, 如果 $A^2 = I$.

首先我们要研究 K 的特征数 $\neq 2$ 的情形. 在 §4 ~ §7 中我们都假定 K 的特征数 $\neq 2$.

定理 1　每个对合在 $SL_n(K)$ 之下都相似于

(1)
$$[1, 1, \cdots, 1, -1, -1, \cdots, -1].$$

【证】 设 $A^2 = I$. 令

$$B = A + I, \quad C = A - I,$$

则

$$O = A^2 - I = BC = CB.$$

设 B 之秩为 r, 则 $0 < r < n$, 因否则我们就有 $A = -I$ 或 $C = 0$ 而 $A = I$. 依定理 2.1, 我们有 $T \in SL_n(K)$, 使得

$$TBT^{-1} = B_1 = \begin{pmatrix} B_{11}^{(rr)} & B_{12}^{(r\ n-r)} \\ 0 & 0 \end{pmatrix}.$$

令 $TCT^{-1} = C_1$, 因 $B - C = 2I$, 我们有 $B_1 - C_1 = 2I$, 于是

$$C_1 = \begin{pmatrix} B_{11} - 2I & B_{12} \\ 0 & -2I \end{pmatrix}.$$

由 $C_1 B_1 = 0$, 可得

$$(B_{11} - 2I)(B_{11}^{(rr)} B_{12}^{(r\ n-r)}) = 0.$$

因为 (B_{11}, B_{12}) 之秩为 r, 所以 $B_{11} - 2I = 0$, 即 $B_{11} = 2I$, 于是我们可以选取 $P^{(r\ n-r)}$, 使得

$$B_2 = \begin{pmatrix} I & P \\ 0 & I \end{pmatrix} B_1 \begin{pmatrix} I & P \\ 0 & I \end{pmatrix}^{-1} = \begin{pmatrix} 2I & -2P + B_{12} \\ 0 & 0 \end{pmatrix}$$
$$= \begin{pmatrix} 2I & 0 \\ 0 & 0 \end{pmatrix},$$

于是

$$A_2 = \begin{pmatrix} I & P \\ 0 & I \end{pmatrix} TAT^{-1} \begin{pmatrix} I & P \\ 0 & I \end{pmatrix}^{-1}$$

$$= \begin{pmatrix} I & P \\ 0 & I \end{pmatrix} T(B-I)T^{-1} \begin{pmatrix} I & P \\ 0 & I \end{pmatrix}^{-1}$$

$$= B_2 - I = \begin{pmatrix} I^{(r)} & 0 \\ 0 & -I^{(n-r)} \end{pmatrix}.$$

定义 2　相似于 (1) 的对合称为 $(r, n-r)$ 对合, 如其中 1 的个数是 r.

显然, 任意两个 $(r, n-r)$ 对合在 $SL_n(K)$ 之下都相似.

由定理 1 可知 V_n 中的行向量在 $(r, n-r)$ 对合 A 之下不变者组成 r 维的子空间, 称为 A 的加空间, 记为 P_A, 而 V_n 中的行向量在 A 之下变号者组成一个 $n-r$ 维子空间, 称为 A 的减空间, 记为 M_A.P_A 和 M_A 是 V_n 的互补空间, 因此 A 的标准形式 (1) 唯一确定. 反之, V_n 的任意一种互补空间唯一地决定两个对合, 以这两个空间为其加空间及减空间, 而这两个对合只差一个符号.

现在我们来研究互相交换的对合.

定理 2　在 $SL_n(K)$ 之下, 一组两两互相交换的对合可以同时化为

$$[e_1, e_2, \cdots, e_n],$$

而 $e_i = \pm 1$.

【证】　假定其中之一化到了

$$\begin{pmatrix} I_1 & 0 \\ 0 & -I_2 \end{pmatrix}. \tag{2}$$

与 (2) 交换的矩阵 A 的形状是

$$A = \begin{pmatrix} A_1 & 0 \\ 0 & A_2 \end{pmatrix}.$$

如果 A 是对合, 即 $A^2 = I$, 则 $A_1^2 = I_1, A_2^2 = I_2$. 依定理 1, 有矩阵 T_1 及 T_2, 使得

$$T_1 A_1 T_1^{-1} = \begin{pmatrix} I_{11} & 0 \\ 0 & -I_{12} \end{pmatrix},$$

$$T_2 A_2 T_2^{-1} = \begin{pmatrix} I_{21} & 0 \\ 0 & -I_{22} \end{pmatrix}$$

可是

$$\begin{pmatrix} T_1 & 0 \\ 0 & T_2 \end{pmatrix} \begin{pmatrix} I_1 & 0 \\ 0 & -I_2 \end{pmatrix} \begin{pmatrix} T_1 & 0 \\ 0 & T_2 \end{pmatrix}^{-1} = \begin{pmatrix} I_1 & 0 \\ 0 & -I_2 \end{pmatrix},$$

因此我们把两个互相交换的对合化到了定理所要求的形状, 如此继续下去, 就可以证明定理.

定理 3　一共有 2^n-2 个互相交换的对合, 在 $SL_n(K)$ 之下以及在 $GL_n(K)$ 之下, 它们组成 $n-1$ 个共轭元素集. 由 $(r,n-r)$ 对合所组成的共轭元素集恰由 $\begin{pmatrix} n \\ r \end{pmatrix}$ 个对合组成.

【证】　只要证明如果 $r\neq r'$, 则 $(r,n-r)$ 对合决不与 $(r',n-r')$ 对合相似就行了. 但这是显然的, 因为它们的加空间的维数不相等.

定理 4　设 J_1 和 J_2 为两交换对合, 则

$$P_{J_1}=(P_{J_1}\cap P_{J_2})\cup(P_{J_1}\cap M_{J_2})$$

及

$$M_{J_1}=(M_{J_1}\cap P_{J_2})\cup(M_{J_1}\cap M_{J_2}).$$

定义 3　由 $GL_n(K)$ 中对合所生成的群, 记作 $SL_n^{\pm}(K)$. 将 $SL_n^{\pm}(K)$ 中差一个 K 中中心元素的元素视为同一, 则得到 $PSL_n^{\pm}(K)$.

定理 5　$SL_n^{\pm}(K)$ 是 $GL_n(K)$ 的特性子群, $SL_n(K)$ 是 $SL_n^{\pm}(K)$ 的特性子群.

【证】　第一个断言显然成立, 现要证第二个断言. 我们先注意 $SL_n^{\pm}(K)$ 是 $GL_n(K)$ 的非中心正规子群, 因之由定理 3.3 可知 $SL_n^{\pm}(K)\supseteq SL_n(K)$, 即 $SL_n(K)$ 是 $SL_n^{\pm}(K)$ 的子群, 除非 $n=2$ 而 K 只有三个元素. 又因 $SL_n(K)$ 是 $GL_n(K)$ 的换位子群, 且是它自己的换位子群, 除非 $n=2$ 及 K 只有三个元素, 所以它也是 $SL_n^{\pm}(K)$ 的换位子群, 因而是 $SL_n^{\pm}(K)$ 的特性子群.

当 $n=2$ 而 K 只有三个元素时, 本定理也成立, 如在第二章定理 4.6 所证明的.

定理 6　如果 -1 属于 K 的乘法群的换位子群 C, 则 $SL_n(K)=SL_n^{\pm}(K)$. 否则, $SL_n(K)$ 在 $SL_n^{\pm}(K)$ 中的指数是 2, 而 $SL_n^{\pm}(K)$ 可以从 $SL_n(K)$ 添加任一个 $(r,n-r)$ 对合 (而 $n-r$ 为奇数) 得到.

【证】　如果 $-1\in C$, 则对任意 $(r,n-r)$ 对合 A, 有

$$\Delta_n(A)=\varphi((-1)^{n-r})=1,$$

于是 $A\in SL_n(K)$, 因此 $SL_n^{\pm}(K)\subseteq SL_n(K)$, 所以 $SL_n(K)=SL_n^{\pm}(K)$.

如果 $-1\notin C$, 则对于任意 $(r,n-r)$ 对合 A 而 $n-r$ 为奇数, 我们有

$$\Delta_n(A)=\varphi((-1)^{n-r})=\varphi(-1)\neq 1,$$

因此

$$SL_n^{\pm}(K)/SL_n(K)\cong\{1,\varphi(-1)\},$$

而 $\{1,\varphi(-1)\}$ 为二阶巡回群, 因此 $SL_n^{\pm}(K):SL_n(K)=2$.

§5 $SL_n(K)$, $SL_n^{\pm}(K)$ 和 $GL_n(K)$ 的自同构 (特征数 $\neq 2$)

引理 $SL_n(K)$ 的自同构必将 $(n-2,2)$ 对合映到 $(n-2,2)$ 对合.

【证】 设 $\mathscr{A}$ 是 $SL_n(K)$ 的一个自同构. 依定理 4.3, $\mathscr{A}$ 必将 $(n-2,2)$ 对合映到 $(n-2,2)$ 对合或 $(2,n-2)$ 对合. 我们进而证明后一情形不可能发生, 除非 $n=4$, 这时 $(n-2,2)$ 对合和 $(2,n-2)$ 对合都是 $(2,2)$ 对合.

当 $n=3$ 时, 考虑 (1, 2) 对合

$$J_1=[-1,-1,1], J_2=[1,-1,-1],$$

它们互相交换, 而且它们的积 $J_1J_2=[-1,1,-1]$ 也是 (1, 2) 对合. 但是两个互相交换的 (2, 1) 对合之积都是 (1, 2) 对合, 因此 $\mathscr{A}$ 只能将 (1, 2) 对合映到 (1, 2) 对合.

当 $n=5$ 时, 我们有两个互相交换的 (3, 2) 对合

$$J_1=[-1,-1,1,1,1], J_2=[1,-1,-1,1,1],$$

它们的乘积 J_1J_2 仍是 (3, 2) 对合. 但是任意两个互相交换的 (2, 3) 对合之积不再是 (2, 3) 对合, 因此 $\mathscr{A}$ 不能将 (3, 2) 对合映到 (2, 3) 对合.

当 $n\geqslant 7$ 时, 可仿 $n=5$ 的情形讨论之.

最后研究 $n=6$ 的情形. 考虑

$$\begin{aligned}
&J_1=[-1,-1,1,1,1,1], \quad J_2=[-1,1,-1,1,1,1],\\
&J_3=[1,-1,-1,1,1,1], \quad J_4=[-1,1,1,1,1,-1],\\
&J_5=[1,-1,1,1,1,-1],
\end{aligned}$$

它们是两两互相交换的 (4, 2) 对合, 具有性质 $J_1J_2=J_3$ 和 $J_1J_4=J_5$. 设 $\mathscr{A}$ 将 (4, 2) 对合映到 (2, 4) 对合, 则 $\mathscr{A}(J_1)$, $\mathscr{A}(J_2)$, $\mathscr{A}(J_3)$, $\mathscr{A}(J_4)$, $\mathscr{A}(J_5)$ 是两两互相交换的 (2, 4) 对合. 因 $\mathscr{A}(J_1)\mathscr{A}(J_2)=\mathscr{A}(J_3)$, $\mathscr{A}(J_1)\mathscr{A}(J_4)=\mathscr{A}(J_5)$, 所以可以设

$$\begin{aligned}
\mathscr{A}(J_1)&=[1,1,-1,-1,-1,-1],\\
\mathscr{A}(J_2)&=[-1,-1,1,1,-1,-1],\\
\mathscr{A}(J_3)&=[-1,-1,-1,-1,1,1],\\
\mathscr{A}(J_4)&=[-1,-1,1,-1,1,-1]\\
&\quad \text{或}[-1,-1,1,-1,-1,1],\\
&\quad \text{或}[-1,-1,-1,1,1,-1],\\
&\quad \text{或}[-1,-1,-1,1,-1,1],
\end{aligned}$$

无论在哪一情形, $\mathscr{A}(J_2)\mathscr{A}(J_4)$ 都是 (4, 2) 对合; 可是由 $J_2J_4=[1,1,-1,1,1,-1]$ 为 (4, 2) 对合推出 $\mathscr{A}(J_2)\mathscr{A}(J_4)$ 应为 (2, 4) 对合, 我们得到一个矛盾.

这样引理就完全证明.

定理 1　设 $n \geqslant 3$. $SL_n(K)$ 的每个自同构或为形状

(I)
$$A \to PA^{\sigma}P^{-1},$$

其中 σ 为 K 之自同构, 而 P 为可逆矩阵; 或为形状

(II)
$$A \to P(A^{\tau'})^{-1}P^{-1},$$

其中 τ 为 K 之反自同构.

【证】　我们对 n 用归纳法来证明本定理.

(i) 先研究 $n=3$ 的情形. 设 $\mathscr{A}$ 是 $SL_3(K)$ 的一个自同构,

$$X \to \mathscr{A}(X).$$

令

$$J_{12}=[-1,-1,1], J_{23}=[1,-1,-1],$$

则 J_{12} 和 J_{23} 是两个互相交换的 (1, 2) 对合, 依引理, $\mathscr{A}(J_{12})$ 和 $\mathscr{A}(J_{23})$ 也是两个互相交换的 (1, 2) 对合. 依定理 4.2, 有 $A \in GL_3(K)$,
使

$$A\mathscr{A}(J_{12})A^{-1}=J_{12}, \quad A\mathscr{A}(J_{23})A^{-1}=J_{23}.$$

那么, 使 $\mathscr{A}$ 承受形如 (I) 的自同构

$$X \to AXA^{-1}$$

之后, 可以假定

(1)
$$\mathscr{A}(J_{12})=J_{12}, \quad \mathscr{A}(J_{23})=J_{23}.$$

$SL_3(K)$ 中与 J_{12} 交换的对合生成一群 $\sum$, 它由一切形状

$$\begin{pmatrix} Q^{(2)} & 0 \\ 0 & \pm 1 \end{pmatrix}, \quad Q^{(2)} \in SL_2^{\pm}(K), \text{而} \det Q^{(2)} \cdot \varphi(\pm 1)=1$$

的元素所组成. 考虑由一切形状

$$\begin{pmatrix} R^{(2)} & 0 \\ 0 & 1 \end{pmatrix} \quad (R^{(2)} \in SL_2(K))$$

的元素所组成的群 Π. 当 $K \neq F_3$ 时, Π 是 $\sum$ 的换位子群; 当 $K=F_3$ 时, 则 Π 是 $\sum$ 中 3 阶元素所生成的群, 自然有 $\mathscr{A}(\sum)=\sum$, 因此 $\mathscr{A}(\Pi)=\Pi$. 同样, 由

$\mathscr{A}(J_{23}) = J_{23}$, 可推得 $\mathscr{A}(\Lambda) = \Lambda$, 这里 Λ 是由一切形状

$$\begin{pmatrix} 1 & 0 \\ 0 & R^{(2)} \end{pmatrix} \quad (R^{(2)} \in SL_2(K))$$

的元素所生成的群.

研究

$$S_{12} = \begin{pmatrix} 0 & 1 & \\ -1 & 0 & \\ & & 1 \end{pmatrix}$$

在 $\mathscr{A}$ 之下的像. 由 $S_{12} \in \Pi$, 可设

$$\mathscr{A}(S_{12}) = \begin{pmatrix} a & b & \\ c & d & \\ & & 1 \end{pmatrix}.$$

由 $S_{12}^2 = J_{12}$, 所以 $(\mathscr{A}(S_{12}))^2 = J_{12}$, 即

(2) $$a^2 + bc = cb + d^2 = -1,$$
$$ab + bd = ca + dc = 0.$$

又因 $S_{12}J_{23}$ 为 2 阶元素, 所以

(3) $$a^2 - bc = -cb + d^2 = 1,$$
$$-ab + bd = ca - dc = 0.$$

由 (2) 及 (3) 推出 $a = d = 0$, $bc = -1$. 使 $\mathscr{A}$ 承受形如 (I) 的自同构

$$X \to \begin{pmatrix} 1 & & \\ & b & \\ & & 1 \end{pmatrix} X \begin{pmatrix} 1 & & \\ & b & \\ & & 1 \end{pmatrix}^{-1}$$

(注意此自同构不变 J_{12}, J_{23}) 之后, 可以假定

(4) $$\mathscr{A}(S_{12}) = S_{12}.$$

研究

$$S_{23} = \begin{pmatrix} 1 & & \\ & 0 & 1 \\ & -1 & 0 \end{pmatrix}$$

在 $\mathscr{A}$ 之下的像, 用同样的方法使 $\mathscr{A}$ 承受 (I) 形的自同构之后, 可以假定

(5) $$\mathscr{A}(S_{23}) = S_{23}.$$

再研究

$$T_{12}=\begin{pmatrix}1&1&\\0&1&\\&&1\end{pmatrix}$$

在 $\mathscr{A}$ 之下的像. 由 $T_{12}\in\Pi$, 可设

$$\mathscr{A}(T_{12})=\begin{pmatrix}a_1&b_1&\\c_1&d_1&\\&&1\end{pmatrix}.$$

由 $(T_{12}J_{23})^2=I$, 推知

$$\begin{pmatrix}a_1&-b_1\\c_1&-d_1\end{pmatrix}^2=\begin{pmatrix}1&0\\0&1\end{pmatrix},$$

即

$$(6)\qquad \begin{aligned}a_1^2-b_1c_1=-c_1b_1+d_1^2=1,\\-a_1b_1+b_1d_1=c_1a_1-d_1c_1=0\end{aligned}.$$

再由 $T_{12}S_{23}$ 为 4 阶元素推知

$$\mathscr{A}(T_{12})S_{23}=\begin{pmatrix}a_1&0&b_1\\c_1&0&d_1\\0&-1&0\end{pmatrix}$$

为 4 阶元素, 因之

$$(7)\qquad \begin{aligned}&\begin{pmatrix}a_1^4-b_1c_1a_1-a_1b_1c_1&-a_1^2b_1+b_1d_1&a_1^3b_1-b_1c_1b_1-a_1b_1d_1\\c_1a_1^3-d_1c_1a_1-c_1b_1c_1&-c_1a_1b_1+d_1^2&c_1a_1^2b_1-d_1c_1b_1-c_1b_1d_1\\-c_1a_1^2+d_1c_1&c_1b_1&-c_1a_1b_1+d_1^2\end{pmatrix}\\&=\begin{pmatrix}1&0&0\\0&1&0\\0&0&1\end{pmatrix}.\end{aligned}$$

由 (7) 推知 $c_1b_1=0$, 于是由 (6) 推知 $a_1^2=d_1^2=1$. 但 b_1,c_1 不能全为 0, 因为否则 $\mathscr{A}(T_{12})$ 将为 2 阶元素或 1 阶元素 $[\pm1,\pm1,1]$, 可是 T_{12} 却不是 2 阶元素也不是 1 阶元素, 因此 $b_1\neq0$ 而 $c_1=0$ 或 $c_1\neq0$ 而 $b_1=0$. 因由 (7) 式中 $-a_1^2b_1+b_1d_1=0$ 或 $-c_1a_1^2+d_1c_1=0$ 推知 $a_1^2=d_1$, 因之 $d_1=1$. 再由 (6) 式中 $-a_1b_1+b_1d_1=0$ 或

$c_1a_1 - d_1c_1 = 0$ 推知 $a_1 = d_1 = 1$, 因之

$$\mathscr{A}(T_{12}) = \begin{pmatrix} 1 & b_1 & \\ & 1 & \\ & & 1 \end{pmatrix} \quad \text{或} \quad \begin{pmatrix} 1 & & \\ c_1 & 1 & \\ & & 1 \end{pmatrix}$$

最后, 再由 $S_{12}T_{12}$ 为 3 阶元素推知 $b_1 = 1$ 而 $c_1 = -1$. 分别研究这两种情形.

(i-1) 设

$$\mathscr{A}(T_{12}) = T_{12}. \tag{8}$$

研究

$$T_{13} = \begin{pmatrix} 1 & & 1 \\ & 1 & \\ & & 1 \end{pmatrix} \quad \text{及} \quad T_{23} = \begin{pmatrix} 1 & & \\ & 1 & 1 \\ & & 1 \end{pmatrix}$$

在 $\mathscr{A}$ 之下的像. 因 $S_{23}^{-1}T_{12}S_{23} = T_{13}$及$S_{12}^{-1}T_{13}S_{12} = T_{23}$, 故

$$\mathscr{A}(T_{13}) = T_{13}, \quad \mathscr{A}(T_{23}) = T_{23}. \tag{9}$$

研究

$$T_{12}(x) = \begin{pmatrix} 1 & x & \\ & 1 & \\ & & 1 \end{pmatrix}$$

在 $\mathscr{A}$ 之下的像, $T_{12}(x) \in \Pi$ 而且 $T_{12}(x)$ 与 T_{12} 相交换, 故 $\mathscr{A}(T_{12}(x))$ 的形状为

$$\mathscr{A}(T_{12}(x)) = \begin{pmatrix} a & b & \\ & a & \\ & & 1 \end{pmatrix}.$$

由 $T_{12}(x)$ 与 T_{13} 相交换推出 $a = 1$, 因此

$$\mathscr{A}\begin{pmatrix} 1 & x & \\ & 1 & \\ & & 1 \end{pmatrix} = \begin{pmatrix} 1 & x^\sigma & \\ & 1 & \\ & & 1 \end{pmatrix}, \tag{10}$$

对一切 $x \in K$. 那么考虑

$$\begin{pmatrix} 1 & x & \\ & 1 & \\ & & 1 \end{pmatrix}\begin{pmatrix} 1 & y & \\ & 1 & \\ & & 1 \end{pmatrix} = \begin{pmatrix} 1 & x+y & \\ & 1 & \\ & & 1 \end{pmatrix} \tag{11}$$

在 $\mathscr{A}$ 之下的像推知 $(x+y)^\sigma = x^\sigma + y^\sigma$. 再者, 由

$$\begin{pmatrix} 1 & & x \\ & 1 & \\ & & 1 \end{pmatrix} = S_{23}^{-1}\begin{pmatrix} 1 & x & \\ & 1 & \\ & & 1 \end{pmatrix}S_{23}$$

及

$$\begin{pmatrix} 1 & & \\ & 1 & x \\ & & 1 \end{pmatrix} = S_{12}^{-1} \begin{pmatrix} 1 & & x \\ & 1 & \\ & & 1 \end{pmatrix} S_{12}$$

推出

$$\mathscr{A} \begin{pmatrix} 1 & & x \\ & 1 & \\ & & 1 \end{pmatrix} = \begin{pmatrix} 1 & & x^\sigma \\ & 1 & \\ & & 1 \end{pmatrix}$$

及

$$\mathscr{A} \begin{pmatrix} 1 & & \\ & 1 & x \\ & & 1 \end{pmatrix} = \begin{pmatrix} 1 & & \\ & 1 & x^\sigma \\ & & 1 \end{pmatrix}.$$

于是考虑

$$\begin{pmatrix} 1 & x & \\ & 1 & \\ & & 1 \end{pmatrix}^{-1} \begin{pmatrix} 1 & & \\ & 1 & y \\ & & 1 \end{pmatrix}^{-1} \begin{pmatrix} 1 & x & \\ & 1 & \\ & & 1 \end{pmatrix} \begin{pmatrix} 1 & & \\ & 1 & y \\ & & 1 \end{pmatrix} \tag{12}$$

$$= \begin{pmatrix} 1 & & xy \\ & 1 & \\ & & 1 \end{pmatrix}$$

在 $\mathscr{A}$ 之下的像推知 $(xy)^\sigma = x^\sigma y^\sigma$. 所以 σ 为 K 之自同构. 因 $SL_3(K)$ 由 S_{12}, S_{23} 及 $T_{12}(x)$(x 跑过 K 中一切元素) 所生成, 所以这时定理成立; 这时 $\mathscr{A}$ 的形状为 (I).

(i-2) 设

$$\mathscr{A}(T_{12}) = \begin{pmatrix} 1 & & \\ -1 & 1 & \\ & & 1 \end{pmatrix}.$$

与情形 (i-1) 完全一样, 可以证明

$$\mathscr{A} \begin{pmatrix} 1 & & 1 \\ & 1 & \\ & & 1 \end{pmatrix} = \begin{pmatrix} 1 & & \\ & 1 & \\ -1 & & 1 \end{pmatrix} \quad 和 \quad \mathscr{A} \begin{pmatrix} 1 & & \\ & 1 & 1 \\ & & 1 \end{pmatrix} = \begin{pmatrix} 1 & & \\ & 1 & \\ & -1 & 1 \end{pmatrix}$$

及

$$\mathscr{A} \begin{pmatrix} 1 & x & \\ & 1 & \\ & & 1 \end{pmatrix} = \begin{pmatrix} 1 & & \\ -x^\tau & 1 & \\ & & 1 \end{pmatrix}, \quad \mathscr{A} \begin{pmatrix} 1 & & x \\ & 1 & \\ & & 1 \end{pmatrix} = \begin{pmatrix} 1 & & \\ & 1 & \\ -x^\tau & & 1 \end{pmatrix}$$

和

$$\mathscr{A}\begin{pmatrix} 1 & & \\ & 1 & x \\ & & 1 \end{pmatrix} = \begin{pmatrix} 1 & & \\ & 1 & \\ & -x^\tau & 1 \end{pmatrix},$$

对一切 $x \in K$. 那么考虑 (11) 式双方在 $\mathscr{A}$ 之下的像即可推出 $(x+y)^\tau = x^\tau + y^\tau$, 考虑 (12) 式双方在 $\mathscr{A}$ 之下的像即可推出 $(xy)^\tau = y^\tau x^\tau$, 所以 τ 为 K 之反自同构, 因此这时定理也成立, 这时 $\mathscr{A}$ 的形状为 (II).

(ii) 再研究 $n = 4$ 的情形. 设 $\mathscr{A}$ 是 $SL_4(K)$ 的一个自同构, 令

$$J_{12} = [-1,-1,1,1], \quad J_{23} = [1,-1,-1,1],$$
$$J_{34} = [1,1,-1,-1].$$

它们是互相交换的 (2, 2) 对合, 而其积 $J_{12}J_{23}, J_{23}J_{34}$ 仍是 (2, 2) 对合. 和 $n = 3$ 的情形一样, 使 $\mathscr{A}$ 承受形为 (I) 的一个自同构之后, 可以假定

(13) $$\mathscr{A}(J_{12}) = J_{12}, \quad \mathscr{A}(J_{23}) = J_{23}, \quad \mathscr{A}(J_{34}) = J_{34},$$

$SL_4(K)$ 中与 J_{12} 可交换的元素组成一群 Γ, 它由一切形状

$$\begin{pmatrix} A^{(2)} & 0 \\ 0 & B^{(2)} \end{pmatrix}, \text{而} \det A^{(2)} \det B^{(2)} = 1$$

的元素所组成. Γ 包有一个子群 Σ, 它由一切形状

$$\begin{pmatrix} P^{(2)} & 0 \\ 0 & Q^{(2)} \end{pmatrix}, \text{而} P^{(2)}, Q^{(2)} \in SL_2(K)$$

的元素所组成. 如 $K \neq F_3, \Sigma$ 就是 Γ 的换位子群; 如 $K = F_3, \Sigma$ 就是 Γ 中所有 3 阶元素所生成的群. 由于 $\mathscr{A}(\Gamma) = \Gamma$, 所以 $\mathscr{A}(\Sigma) = \Sigma$. Σ 包有两个子群 Π_1 和 Π_2; Π_1 由一切形状

$$\begin{pmatrix} P^{(2)} & 0 \\ 0 & I^{(2)} \end{pmatrix} \quad (P^{(2)} \in SL_2(K))$$

的元素所组成, 而 Π_2 由一切形状

$$\begin{pmatrix} I^{(2)} & 0 \\ 0 & Q^{(2)} \end{pmatrix} \quad (Q^{(2)} \in SL_2(K))$$

的元素所组成. 分别研究以下诸情形:

1° $K \neq F_3$. 这时 Π_1 和 Π_2 是 Σ 中仅有的两个真正规子群, 而与其换位子群相重者, 所以

$$(14) \qquad \mathscr{A}(\varPi_1)=\varPi_1, \quad \mathscr{A}(\varPi_2)=\varPi_2$$

或

$$\mathscr{A}(\varPi_1)=\varPi_2, \quad \mathscr{A}(\varPi_2)=\varPi_1$$

2° $K=F_3$. 考虑

$$T_{12}=\begin{pmatrix} 1 & 1 & \\ & 1 & \\ & & I^{(2)} \end{pmatrix}$$

在 $\mathscr{A}$ 之下的像. 设

$$\mathscr{A}(T_{12})=\begin{pmatrix} A^{(2)} & \\ & B^{(2)} \end{pmatrix}.$$

因 $T_{12}^3=I$, 故 $A^3=B^3=I$. 如 A, B 皆中心元素, 则有 $A=B=I$, 此为不可能; 如 A,B 皆非中心元素, 则

$$T_{12} \quad 和 \quad \mathscr{A}(T_{12})$$

在 $\varSigma$ 中的中心化子的阶分别为 $6\cdot 24$ 和 $6\cdot 6$, 这也是不可能的. 所以 A 和 B 中有一个是 I 而另一个不是中心元素. 由于 $\varPi_1$ 是 $\varSigma$ 中包有 T_{12} 的最小正规子群, 而 $\varSigma$ 中包有 $\mathscr{A}(T_{12})$ 的最小正规子群或是 $\varPi_1$ 或是 $\varPi_2$. 因之, 这时 (14) 也成立.

进一步, 我们证明 $\mathscr{A}(\varPi_1)=\varPi_2$ 不可能发生. 实际上, 设 $\mathscr{A}(\varPi_1)=\varPi_2$, 研究

$$S_{12}=\begin{pmatrix} 0 & 1 & & \\ -1 & 0 & & \\ & & 1 & \\ & & & 1 \end{pmatrix}$$

在 $\mathscr{A}$ 之下的像, 可设

$$\mathscr{A}(S_{12})=\begin{pmatrix} 1 & & & \\ & 1 & & \\ & & a & b \\ & & c & d \end{pmatrix}.$$

因 $S_{12}^2=J_{12}$, 故 $\mathscr{A}(S_{12}))^2=J_{12}$, 这自然是不可能的. 于是除了 (13) 之外, 我们总有

$$(15) \qquad \mathscr{A}(\varPi_1)=\varPi_1, \quad \mathscr{A}(\varPi_2)=\varPi_2.$$

于是可设

$$\mathscr{A}(S_{12}) = \begin{pmatrix} a & b & & \\ c & d & & \\ & & 1 & \\ & & & 1 \end{pmatrix}.$$

从 $S_{12}^2 = J_{12}, (S_{12}J_{23})^2 = I$ 推出 $a = d = 0, bc = -1$. 于是使 $\mathscr{A}$ 承受形如 (I) 的自同构

$$X \to \begin{pmatrix} 1 & & \\ & b & \\ & & I^{(2)} \end{pmatrix} X \begin{pmatrix} 1 & & \\ & b & \\ & & I^{(2)} \end{pmatrix}^{-1}$$

之后 (注意此自同构不变 J_{12}, J_{23}, J_{34} 及 Π_1, Π_2), 可设

(16) $$\mathscr{A}(S_{12}) = S_{12}.$$

再研究

$$S_{23} = \begin{pmatrix} 1 & & & \\ & 0 & 1 & \\ & -1 & 0 & \\ & & & 1 \end{pmatrix}$$

在 $\mathscr{A}$ 之下的像. 因 S_{23} 与 J_{23} 交换, 故可设

$$\mathscr{A}(S_{23}) = \begin{pmatrix} a & & & b \\ & e & f & \\ & g & h & \\ c & & & d \end{pmatrix}.$$

因 $S_{23}^2 = J_{23}, (S_{23}J_{12})^2 = I$, 所以

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix}^2 = I, \quad \begin{pmatrix} e & f \\ g & h \end{pmatrix}^2 = I,$$
$$\begin{pmatrix} -a & b \\ -c & d \end{pmatrix}^2 = I, \quad \begin{pmatrix} -e & f \\ -g & h \end{pmatrix}^2 = I,$$

即

$$\begin{aligned} &a^2 + bc = 1, && ab + bd = 0, && ca + dc = 0, && cb + d^2 = 1, \\ &a^2 - bc = 1, && -ab + bd = 0, && ca - dc = 0, && -cb + d^2 = 1, \\ &e^2 + fg = -1, && ef + fh = 0 && ge + hg = 0 && gf + h^2 = -1, \\ &e^2 - fg = 1, && -ef + fh = 0, && ge - hg = 0, && -gf + h^2 = 1. \end{aligned}$$

由此推出 $a^2=d^2=1, b=c=0, e=h=0, fg=-1$. 使 $\mathscr{A}$ 承受形如 (I) 的自同构

$$X \to \begin{pmatrix} 1 & & & \\ & 1 & & \\ & & f & \\ & & & 1 \end{pmatrix} X \begin{pmatrix} 1 & & & \\ & 1 & & \\ & & f & \\ & & & 1 \end{pmatrix}^{-1}$$

之后, 除了 (12), (14), (15) 以外, 还可设

$$\mathscr{A}(S_{23}) = \begin{pmatrix} a & & & \\ & 0 & 1 & \\ & -1 & 0 & \\ & & & d \end{pmatrix},$$

而 $a^2=d^2=1$. 又由 $(S_{12}S_{23})^3=I$ 可推出 $a=d=1$. 因之

(17) $$\mathscr{A}(S_{23}) = S_{23}.$$

根据同样的道理, 还可以假定

(18) $$\mathscr{A}(S_{34}) = S_{34},$$

而 $$S_{34} = \begin{pmatrix} 1 & & & \\ & 1 & & \\ & & 0 & 1 \\ & & -1 & 0 \end{pmatrix}.$$

再研究 T_{12} 在 $\mathscr{A}$ 之下的像. 因 $T_{12} \in \Pi_1$, 故可设

$$\mathscr{A}(T_{12}) = \begin{pmatrix} a & b & & \\ c & d & & \\ & & 1 & \\ & & & 1 \end{pmatrix},$$

于是和 $n=3$ 的情形一样, 从关系式 $(T_{12}J_{23})^2=I, (T_{12}S_{23})^4=I$ 及 $(S_{12}T_{12})^2=I$ 推出 $a=d=1, bc=0, b=1$ 或 $c=-1$. 因之

$$\mathscr{A}(T_{12}) = \begin{pmatrix} 1 & 1 & & \\ & 1 & & \\ & & 1 & \\ & & & 1 \end{pmatrix} \quad 或 \quad \begin{pmatrix} 1 & & & \\ -1 & 1 & & \\ & & 1 & \\ & & & 1 \end{pmatrix}.$$

分别研究这两种情形.

(ii-1) 设

(19)
$$\mathscr{A}(T_{12}) = T_{12}.$$
则由
$$T_{13} = S_{23}^{-1}T_{12}S_{23}, \quad T_{23} = S_{12}^{-1}T_{13}S_{12},$$
$$T_{24} = S_{34}^{-1}T_{23}S_{34}, \quad T_{34} = S_{23}^{-1}T_{24}S_{23}$$
推出
(20)
$$\mathscr{A}(T_{13}) = T_{13}, \quad \mathscr{A}(T_{23}) = T_{23},$$
$$\mathscr{A}(T_{24}) = T_{24}, \quad \mathscr{A}(T_{34}) = T_{34}.$$

研究
$$T_{12}(x) = \begin{pmatrix} 1 & x & & \\ & 1 & & \\ & & 1 & \\ & & & 1 \end{pmatrix}$$
在 $\mathscr{A}$ 之下的像. 由于 $T_{12}(x) \in \Pi_1, T_{12}(x)$ 与 T_{12}, T_{13} 皆可换, 和 $n=3$ 的情形一样, 有
$$\mathscr{A}(T_{12}(x)) = \begin{pmatrix} 1 & x^\sigma & & \\ & 1 & & \\ & & 1 & \\ & & & 1 \end{pmatrix}.$$
用 $n=3$ 的情形一样的方法可证 σ 是 K 的自同构, 这时, $\mathscr{A}$ 是形如 (I) 的自同构.

(ii-2) 设

(21)
$$\mathscr{A}(T_{12}) = \begin{pmatrix} 1 & & & \\ -1 & 1 & & \\ & & 1 & \\ & & & 1 \end{pmatrix}.$$
与情形 (ii-1) 相仿, 可证
$$\mathscr{A}(T_{13}) = \begin{pmatrix} 1 & & & \\ & 1 & & \\ -1 & & 1 & \\ & & & 1 \end{pmatrix}, \quad \mathscr{A}(T_{23}) = \begin{pmatrix} 1 & & & \\ & 1 & & \\ & -1 & 1 & \\ & & & 1 \end{pmatrix},$$
$$\mathscr{A}(T_{24}) = \begin{pmatrix} 1 & & & \\ & 1 & & \\ & & 1 & \\ & -1 & & 1 \end{pmatrix}, \quad \mathscr{A}(T_{34}) = \begin{pmatrix} 1 & & & \\ & 1 & & \\ & & 1 & \\ & & -1 & 1 \end{pmatrix}$$
及
$$\mathscr{A}(T_{12}(x)) = T_{21}(-x^\tau),$$

其中 τ 为 K 之反自同构. 这时, $\mathscr{A}$ 是形如 (II) 的自同构.

(iii)$n \geqslant 5$. 设 $\mathscr{A}$ 为 $SL_n(K)$ 的自同构. 考虑

$$J_{n-1,n} = [1, \cdots, 1, -1, -1], \quad J_{1n} = [-1, 1, \cdots, 1, -1],$$

它们是两个互相交换的 $(n-2, 2)$ 对合, 其积也为 $(n-2, 2)$ 对合, 因此, 使 $\mathscr{A}$ 承受一个形如 (I) 的自同构之后, 可设

$$\mathscr{A}(J_{n-1,n}) = J_{n-1,n}, \quad \mathscr{A}(J_{1n}) = J_{1n}. \tag{22}$$

$SL_n(K)$ 中与 $J_{n-1,n}$ 交换的元素组成一群 Γ_1, Γ_1 由一切形状

$$\begin{pmatrix} P^{(n-2)} & 0 \\ 0 & Q^{(2)} \end{pmatrix}, \text{而} \det P^{(n-2)} \det Q^{(2)} = 1$$

的元素所组成. 将 Γ_1 的换位子群记作 Σ_1, 则 Σ_1 由一切形状

$$\begin{pmatrix} A^{(n-2)} & 0 \\ 0 & B^{(2)} \end{pmatrix}, \text{而} A^{(n-2)} \in SL_{n-2}(K), B^{(2)} \in SL_2(K)$$

的元素所组成. 显然, $\mathscr{A}(\Gamma_1) = \Gamma_1, \mathscr{A}(\Sigma_1) = \Sigma_1$.

Σ_1 包有两个正规子群 Π_1 和 Π_2. Π_1 由一切形状

$$\begin{pmatrix} R_1^{(n-2)} & 0 \\ 0 & I^{(2)} \end{pmatrix} \quad (R_1^{(n-2)} \in SL_{n-2}(K))$$

的元素组成; 而 Π_2 由一切形状

$$\begin{pmatrix} I^{(n-2)} & 0 \\ 0 & S_1^{(2)} \end{pmatrix} \quad (S_1^{(2)} \in SL_2(K))$$

的元素所组成. Π_1 和 Π_2 是 Σ_1 中仅有的两个真正规子群而与其换位子群相重者. 又因 $n \geqslant 5, n-2 > 2$, 故 $\Pi_1(\cong SL_{n-2}(K))$ 与 $\Pi_2(\cong SL_2(K))$ 中所含两两交换的对合的最大个数不等, 所以它们不可能同构, 因此一定有

$$\mathscr{A}(\Pi_1) = \Pi_1.$$

从 J_{1n} 出发, 得出 $\mathscr{A}$ 将群 Δ_1 不变, 而 Δ_1 由一切形状

$$\begin{pmatrix} 1 & & \\ & R_2^{(n-2)} & \\ & & 1 \end{pmatrix} \quad (R_2^{(n-2)} \in SL_{n-2}(K))$$

的元素所组成. Π_1 和 Δ_1 生成一群 Π, 它由一切形状

$$\begin{pmatrix} R^{(n-1)} & \\ & 1 \end{pmatrix} \quad (R^{(n-1)} \in SL_{n-1}(K))$$

的元素所组成. 于是

$$\mathscr{A}\begin{pmatrix} R^{(n-1)} & \\ & 1 \end{pmatrix} = \begin{pmatrix} \mathscr{A}_1(R^{(n-1)}) & \\ & 1 \end{pmatrix},$$

而 $\mathscr{A}_1$ 为 $SL_{n-1}(K)$ 的自同构. 依归纳法假设,

$$\mathscr{A}_1(R) = PR^{\sigma}P^{-1} \tag{23}$$

或

$$\mathscr{A}_1(R) = P(R^{\tau'})^{-1}P^{-1}, \tag{24}$$

因此, 使 $\mathscr{A}$ 承受形如 (I) 的自同构

$$X \to \left[\begin{pmatrix} P & \\ & 1 \end{pmatrix}^{-1} X \begin{pmatrix} P & \\ & 1 \end{pmatrix}\right]^{\sigma^{-1}}$$

(如 (23) 发生), 或形状 (II) 的自同构

$$X \to \left\{\left[\begin{pmatrix} P & \\ & 1 \end{pmatrix}^{-1} X \begin{pmatrix} P & \\ & 1 \end{pmatrix}^{\tau^{-1\prime}}\right]\right\}^{-1}$$

(如 (24) 发生) 之后, 可设

$$\mathscr{A}\begin{pmatrix} R & \\ & 1 \end{pmatrix} = \begin{pmatrix} R & \\ & 1 \end{pmatrix}, \text{对一切} R \in SL_{n-1}(K). \tag{25}$$

最后来研究元素

$$S_{n-1,n} = \begin{pmatrix} I^{(n-2)} & & \\ & 0 & 1 \\ & -1 & 0 \end{pmatrix}$$

在 $\mathscr{A}$ 之下的像. 因 $S_{n-1,n}$ 与 Π 中每个元素皆交换, 而 Π 中每个元素在 $\mathscr{A}$ 之下皆不变, 故可设

$$\mathscr{A}(S_{n-1,n}) = \begin{pmatrix} \rho I^{(n-2)} & & \\ & a & b \\ & c & d \end{pmatrix},$$

其中 ρ 为 K 的非零中心元素. 因 $S_{n-1,n}^2 = J_{n-1,n}$ 及 $(S_{n-2,n-1}S_{n-1,n})^3 = I$, 而 $J_{n-1,n}$ 和 $S_{n-2,n-1}$ 在 $\mathscr{A}$ 之下皆不变, 故 $(\mathscr{A}(S_{n-1,n}))^2 = J_{n-1,n}$,

$(S_{n-1,n-2}\mathscr{A}(S_{n-1,n}))^3 = I$, 由此推出 $\rho = 1, a = d = 0, bc = -1$. 于是使 $\mathscr{A}$ 承受形如 (I) 的自同构

$$X \to \begin{pmatrix} I^{(n-1)} & \\ & b \end{pmatrix} X \begin{pmatrix} I^{(n-1)} & \\ & b \end{pmatrix}^{-1} \tag{26}$$

之后, 可设

$$\mathscr{A}(S_{n-1,n}) = S_{n-1,n}.$$

因 (26) 不变 Π 中元素, 而 $SL_n(K)$ 由 Π 及 $S_{n-1,n}$ 生成, 故

$$\mathscr{A}(X) = X,$$

对一切 $X \in SL_n(K)$. 因此定理当 $n \geqslant 5$ 时也成立.

定理 1 至此完全证毕.

以下定理是定理 1 的直接推论.

定理 2　$GL_n(K)$(或 $SL_n^{\pm}(K)$) 的每个自同构或为

$$\text{I.} \qquad A \to \chi(A)PA^{\sigma}P^{-1},$$

其中 σ 为 K 之自同构, P 为可逆矩阵, χ 为 $GL_n(K)$(或 $SL_n^{\pm}(K)$) 到 K 中心的乘法群中的一个同态; 或为

$$\text{II.} \qquad A \to \chi(A)P(A^{\tau'})^{-1}P^{-1},$$

其中 τ 为 K 之反自同构.

【证】　$n = 2$ 的情形在第二章中已经证过了, 现在我们来研究 $n \geqslant 3$ 的情形.

设 $\mathscr{A}$ 为 $GL_n(K)$(或 $SL_n^{\pm}(K)$) 的自同构. 因为当 $n \geqslant 3$ 时, $SL_n(K)$ 是 $GL_n(K)$(或 $SL_n^{\pm}(K)$) 的换位子群, 所以 $\mathscr{A}$ 将 $SL_n(K)$ 不变, 因而诱导出 $SL_n(K)$ 的一个自同构. 依定理 1, 使 $\mathscr{A}$ 承受一个形如 I 或 II 的自同构之后, 可以假定

$$\mathscr{A}(A) = A \quad (A \in SL_n(K)). \tag{27}$$

$GL_n(K)$(或 $SL_n^{\pm}(K)$) 中任一元素 X 皆可表示

$$X = AD(\mu),$$

其中 $A \in SL_n(K)$ 而 $D(\mu) = [1, \cdots, 1, \mu]$(或 $D(\mu) = [1, \cdots, 1, \pm 1]$), 因此只要求 $D(\mu)$ 在 $\mathscr{A}$ 之下的像就行了.

假定

$$\mathscr{A}(D(\mu)) = C,$$

因 $D(\mu)AD(\mu)^{-1} \in SL_n(K)$ 对所有 $A \in SL_n(K)$, 故由 (27) 得

$$D(\mu)AD(\mu)^{-1} = CAC^{-1},$$

即

$$AD(\mu)^{-1}C = D(\mu)^{-1}CA,$$

对所有 $A \in SL_n(K)$, 自然有

$$D(\mu)^{-1}C = \rho I,$$

而 $\rho \in K$ 之中心, 定理得证.

§6 射影对合 (特征数 $\neq 2$)

可逆矩阵 A 所诱导出来的射影变换记作 $\overline{A}$. 显然, $\overline{A} = \overline{B}$ 当且仅当有 K 之中心元素 γ, 使得 $A = \gamma B$.

$PGL_n(K)$ 中 (或 $PSL_n(K)$ 中) 一对元素 $\overline{A}$ 和 $\overline{B}$ 称为在 $PGL_n(K)$(或 $PSL_n(K)$) 之下共轭, 如果 $PGL_n(K)$(或 $PSL_n(K)$) 中有一个元素 $\overline{P}$ 使得 $\overline{A} = \overline{P}\,\overline{B}\,\overline{P}^{-1}$. 相当地, 我们有 $A = \alpha PBP^{-1}$, 而 α 为 K 的中心元素.

两个射影变换 $\overline{A}$ 和 $\overline{B}$ 是交换的, 当且仅当 $AB = \gamma BA$, 而 γ 为 K 的中心元素.

定义 1 非中心矩阵 A 称为射影对合, 如果 $A^2 = \gamma I$, 而 γ 属于 K 之中心, γ 称为 A 的数量.

设 A 和 B 为射影对合, 即 $A^2 = \alpha I, B^2 = \beta I$, 而 α 和 β 为中心元素. 如果它们在 $PGL_n(K)$(或 $PSL_n(K)$) 之下共轭, 则有 $P \in PGL_n(K)$(或 $P \in PSL_n(K)$), 使得

$$A = \gamma PBP^{-1},$$

而 γ 为中心元素. 于是

$$\alpha I = A^2 = \gamma^2(PBP^{-1})^2 = \gamma^2 PB^2P^{-1} = \gamma^2\beta I,$$

因此 $\alpha = \gamma^2\beta$. 这就证明了两个共轭射影对合只差一个中心元素的平方因子, 因为 B 和 γB 表示同一射影变换, 所以不妨假定共轭对合的数量相同.

我们可以把 $PGL_n(K)$(或 $PSL_n(K)$) 中的射影对合分到在 $PGL_n(K)$(或 $PSL_n(K)$) 之下共轭的一些共轭元素类的集合 Γ_α 里, 而 Γ_α 为由所有具数量 α 的射影对合所组成的集合, 同时 α 跑过 K 的中心的乘法群对它的平方元素的子群的陪集的一组完全代表系的子集合. 当然, 每个集合 Γ_α 可以由几个共轭元素类组成, 可是一个共轭元素类只包在一个集合 Γ_α 里.

如果 A 是射影对合, 即 $A^2=\alpha I$, 而 B 与 A 交换, 则 $AB=BA$ 或 $AB=-BA$. 实际上, 由 $AB=\gamma BA$ 可推出

$$\alpha B=A^2B=\gamma ABA=\gamma^2BA^2=\alpha\gamma^2B.$$

于是 $\gamma^2=1$, 因之 $AB=\pm BA$.

定义 2 Γ_1 中的射影对合称为第一种对合. Γ_γ 中的对合, 如 γ 为 K 中一元素之平方, 但不是 K 中之中心元素之平方, 称为第二种对合. 其余的对合, 即当 γ 不是 K 中元素之平方时, Γ_γ 中之对合称为第三种对合.

以下我们要详细讨论这三种对合. 我们从 Γ_1 开始.

对应于 $GL_n(K)$ 中 $(r,n-r)$ 对合或 $(n-r,r)$ 对合的第一种对合称为 r 对合. 因之我们可以假定 $2r\leqslant n$. 显然, $PGL_n(K)$ 中的第一种对合在 $PGL_n(K)$ 之下以及 $PSL_n(K)$ 之下分到 $\left[\dfrac{n}{2}\right]$ 个 r 对合的集合里.

定理 1 $PGL_n(K)$ 中彼此互相交换的 r 对合的最大个数等于 $\begin{pmatrix} n \\ r \end{pmatrix}$, 如果 $r\neq\dfrac{n}{2}$; 而不小于 $\dfrac{1}{2}\begin{pmatrix} n \\ r \end{pmatrix}$, 如果 $r=\dfrac{n}{2}$.

【证】 设 A 和 B 为 $PGL_n(K)$ 中两个互相交换的 r 对合, 则 $AB=\pm BA$. 如果 $AB=-BA$, 则 A 交换 B 的加空间和减空间, 因之有 $n=2r$, 即 $AB=-BA$ 只在 n 为偶数且 $r=\dfrac{n}{2}$ 时才发生, 于是我们的定理由定理 4.3 推出.

系理 $PGL_n(K)$ 中彼此互相交换的 1 对合的最大个数小于 $PGL_n(K)$ 中彼此互相交换的 r 对合, $r>1$, 的最大个数.

【证】 我们分以下三个情形来讨论:

(i) $r\neq\dfrac{n}{2}$. 因为 $\begin{pmatrix} n \\ r \end{pmatrix}>n$, 对于 $r>1$, 这时我们的定理成立.

(ii) n 为偶数而 $r=\dfrac{n}{2}>2$. 因为

$$\frac{1}{2}\begin{pmatrix} 2r \\ r \end{pmatrix}\geqslant\frac{1}{2}\begin{pmatrix} 2r \\ r \end{pmatrix}=\frac{1}{2}\frac{2r(2r-1)}{1\cdot 2}>2r\quad(\text{若}r>2),$$

故定理也成立.

(iii) $n=4$. 互相交换的 1 对合的个数为 4, 可是我们至少有 5 个互相交换的 2 对合:

$$\begin{pmatrix}1&&&\\&1&&\\&&-1&\\&&&-1\end{pmatrix},\quad\begin{pmatrix}1&&&\\&-1&&\\&&1&\\&&&-1\end{pmatrix},\quad\begin{pmatrix}1&&&\\&-1&&\\&&-1&\\&&&1\end{pmatrix},$$

$$\begin{pmatrix}0&0&1&0\\0&0&0&1\\1&0&0&0\\0&1&0&0\end{pmatrix},\quad\begin{pmatrix}0&0&1&0\\0&0&0&-1\\1&0&0&0\\0&-1&0&0\end{pmatrix},$$

定理也成立.

定理 2 设 $\Gamma_\gamma\neq\Gamma_1$. 如果 $\gamma=\lambda^2$, 而 λ 为 K 之非中心元素, 即 Γ_γ 为第二种对合的集合, 则 Γ_γ 中每个元素在 $PGL_n(K)$ 之中都共轭于

(1) $$[\lambda,\lambda,\cdots,\lambda].$$

如果 $\gamma=\lambda^2$ 在 K 中不可解, 即 Γ_γ 为第三种对合的集合, 则 Γ_γ 中每个元素在 $PGL_n(K)$ 之中都共轭于

(2) $$\begin{pmatrix}0&I\\\gamma I&0\end{pmatrix}.$$

当然, 这个情形只有在 n 为偶数时才能发生.

【证】 我们先来证明: 如果 $\gamma=\lambda^2$ 在 K 中可解, 可是在 K 的中心里不可解, 则 $\gamma=\lambda^2$ 的根在 K 中都互相共轭. 设 λ 和 μ 是 $\gamma=\lambda^2$ 的两个根, 如果 $\lambda\neq-\mu$, 则

$$\lambda(\lambda+\mu)=(\lambda+\mu)\mu;$$

如果 $\lambda=-\mu$, 则有 $v\in K$, 使得 $v\lambda\neq\lambda v$, 于是

$$\lambda(v\lambda-\lambda v)=(v\lambda-\lambda v)(-\lambda).$$

现在我们用归纳法来证明本定理. 设 $A\in\Gamma_\gamma$. 写

$$A=\begin{pmatrix}a_{11}&a_{12}&\cdots&a_{1n}\\a_{21}&a_{22}&\cdots&a_{2n}\\\cdots&\cdots&\cdots&\cdots\\a_{n1}&a_{n2}&\cdots&a_{nn}\end{pmatrix}.$$

如果 $a_{12}=\cdots=a_{1n}=0$, 则由 $A^2=\gamma I$ 推出 $a_{11}^2=\gamma$. 这时, $\gamma=\lambda^2$ 在 K 中可解, 于是 a_{11} 与 λ 在 K 中共轭, 因此不妨设

$$A=\begin{pmatrix}\lambda & 0 & \cdots & 0\\ a_{21} & a_{22} & \cdots & a_{2n}\\ \cdots & \cdots & \cdots & \cdots\\ a_{n1} & a_{n2} & \cdots & a_{nn}\end{pmatrix}.$$

于是

$$\begin{pmatrix}1 & 0 \ \cdots \ 0\\ -\frac{1}{2}a_{21}\lambda^{-1} & \\ \vdots & I\\ -\frac{1}{2}a_{n1}\lambda^{-1} & \end{pmatrix} A \begin{pmatrix}1 & 0 \ \cdots \ 0\\ -\frac{1}{2}a_{21}\lambda^{-1} & \\ \vdots & I\\ -\frac{1}{2}a_{n1}\lambda^{-1} & \end{pmatrix}^{-1}=\begin{pmatrix}\lambda & 0 \ \cdots \ 0\\ 0 & \\ \vdots & A_1\\ 0 & \end{pmatrix},$$

其中 A_1 为 $(n-1)\times(n-1)$ 矩阵而 $A_1^2=\gamma I$. 依归纳法假设, A_1 与

$$[\lambda,\cdots,\lambda]\ \ (\text{共有}n-1\text{个}\lambda)$$

共轭, 因此 A 与 (1) 在 $PGL_n(K)$ 中共轭.

如 $(a_{12},\cdots,a_{1n})\neq 0$, 于是有 $(n-1)\times(n-1)$ 的可逆矩阵 P_1, 使

$$(a_{12},\cdots,a_{1n})P_1=(1,0,\cdots,0),$$

于是

$$\begin{pmatrix}1 & \\ & P_1\end{pmatrix}^{-1} A \begin{pmatrix}1 & \\ & P_1\end{pmatrix}=\begin{pmatrix}a_{11} & 1 & 0 & \cdots & 0\\ & & * & & \end{pmatrix}$$

及

$$\begin{pmatrix}1 & 0 & \\ -a_{11} & 1 & \\ & & I^{(n-2)}\end{pmatrix}^{-1}\begin{pmatrix}a_{11} & 1 & 0 & \cdots & 0\\ & & * & & \end{pmatrix}\begin{pmatrix}1 & 0 & \\ -a_{11} & 1 & \\ & & I^{(n-2)}\end{pmatrix}$$
$$=\begin{pmatrix}0 & 1 & 0 & \cdots & 0\\ & & * & & \end{pmatrix},$$

因此不妨设

$$A=\begin{pmatrix}0 & 1 & 0 & \cdots & 0\\ a_{21} & a_{22} & a_{23} & \cdots & a_{2n}\\ \cdots & \cdots & \cdots & \cdots & \cdots\\ a_{n1} & a_{n2} & a_{n3} & \cdots & a_{nn}\end{pmatrix}.$$

从 $A^2 = \gamma I$ 推出 $a_{21} = \gamma, a_{22} = a_{23} = \cdots = a_{2n} = 0$, 于是

$$A = \begin{pmatrix} 0 & 1 & 0 & \cdots & 0 \\ \gamma & 0 & 0 & \cdots & 0 \\ a_{31} & a_{32} & a_{33} & \cdots & a_{3n} \\ \cdots & \cdots & \cdots & \cdots & \cdots \\ a_{n1} & a_{n2} & a_{n3} & \cdots & a_{nn} \end{pmatrix}.$$

那么

$$\begin{pmatrix} I^{(2)} & \\ -\frac{1}{2}\begin{pmatrix} a_{31} & a_{32} \\ \vdots & \vdots \\ a_{n1} & a_{n2} \end{pmatrix}\begin{pmatrix} 0 & 1 \\ \gamma & 0 \end{pmatrix}^{-1} & I^{(n-2)} \end{pmatrix} A$$

$$\cdot \begin{pmatrix} I^{(2)} & \\ -\frac{1}{2}\begin{pmatrix} a_{31} & a_{32} \\ \vdots & \vdots \\ a_{n1} & a_{n2} \end{pmatrix}\begin{pmatrix} 0 & 1 \\ \gamma & 0 \end{pmatrix}^{-1} & I^{(n-2)} \end{pmatrix}^{-1} = \begin{pmatrix} 0 & 1 & \\ \gamma & 0 & 0 \\ 0 & & A_2 \end{pmatrix},$$

其中 A_2 为 $(n-2) \times (n-2)$ 矩阵而 $A_2^2 = \gamma I$. 如 $\lambda^2 = \gamma$ 在 K 中可解而在 K 的中心中不可解, 设 λ 为一解, 则有 $v \in K$, 使 $v\lambda \neq \lambda v$. 令 $v\lambda - \lambda v = \xi$, 则

$$\begin{pmatrix} 1 & \lambda\gamma^{-1} \\ \lambda\xi & \xi \end{pmatrix}\begin{pmatrix} 0 & 1 \\ \gamma & 0 \end{pmatrix} = \begin{pmatrix} \lambda & 0 \\ 0 & \lambda \end{pmatrix}\begin{pmatrix} 1 & \lambda\gamma^{-1} \\ \lambda\xi & \xi \end{pmatrix}.$$

因为

$$\begin{pmatrix} 1 & \lambda\gamma^{-1} \\ \lambda\xi & \xi \end{pmatrix} = \begin{pmatrix} 2 & \lambda\gamma^{-1} \\ 0 & \xi \end{pmatrix}\begin{pmatrix} 1 & 0 \\ -\lambda & 1 \end{pmatrix},$$

所以它是可逆的, 这证明了 $\begin{pmatrix} 0 & 1 \\ \gamma & 0 \end{pmatrix}$ 与 $\begin{pmatrix} \lambda & 0 \\ 0 & \lambda \end{pmatrix}$ 共轭. 又依归纳法假设, A_2 与

$$[\lambda, \cdots, \lambda] \quad (\text{共} n-2 \text{个} \lambda)$$

共轭, 故这时 A 与 (1) 共轭. 又如 $\lambda^2 = \gamma$ 在 K 中不可解, 仍依归纳法假设, 这时 A_2 与

$$\begin{pmatrix} 0 & I^{(\frac{n-2}{2})} \\ \gamma I^{(\frac{n-2}{2})} & 0 \end{pmatrix}$$

共轭, 而 $n-2$ 为偶. 故这时 A 与 (2) 共轭, 而 n 为偶数.

系理 1　在 $PGL_n(K)$ 中, 每个 $\Gamma_\gamma(\neq \Gamma_1)$ 都只由一个共轭元素类组成.

系理 2　在 $PGL_n(K)$ 中, 第二种对合的集合 Γ_γ 中至少有 2^{n-1} 个互相交换的对合, 因此, $PGL_n(K)$ 中互相交换的 1 对合的最大个数小于第二种对合的集合 Γ_γ 中互相交换的对合的最大个数, 只要 $n \geqslant 3$.

【证】　不失普遍性, 可以假定 Γ_γ 中一组互相交换的对合包有

$$[\lambda, \lambda, \cdots, \lambda],$$

而 $\lambda^2 = \gamma$. 令 $T = [t_1, t_2, \cdots, t_n]$ 而 $t_i = \xi(\xi = v\lambda - \lambda v \neq 0)$ 或 $1(i = 1, 2, \cdots, n)$. 则

$$T[\lambda, \lambda, \cdots, \lambda]T^{-1} = [\pm\lambda, \pm\lambda, \cdots, \pm\lambda]$$

给出 $\dfrac{1}{2}2^n = 2^{n-1}$ 个 Γ_γ 中的互相交换的对合.

如 $n \geqslant 3$, 显然 $2^{n-1} > n$, 因之系理 2 之第二个断言成立.

定理 3　令 $n > 6$. 在 $PGL_n(K)$ 中, 任一第三种对合的集合 Γ_γ 里都有两对互相交换的对合而它们的积在 $PGL_n(K)$ 里不共轭. (可是显然, 两个不同的 1 对合之积为 2 对合.)

【证】　设 J 为 $GL_m(K)$ 中之一 $(r, m-r)$ 对合, $m = \dfrac{n}{2}, r < m$, 则

$$\begin{pmatrix} 0 & J \\ \gamma J & 0 \end{pmatrix}$$

为 Γ_γ 中之对合, 而

$$\begin{pmatrix} 0 & I \\ \gamma I & 0 \end{pmatrix}\begin{pmatrix} 0 & J \\ \gamma J & 0 \end{pmatrix} = \begin{pmatrix} \gamma J & 0 \\ 0 & \gamma J \end{pmatrix}$$

为 $2r$ 对合, 因此, 如 $n > 6$, 即 $n = 2m, m \geqslant 4$, 我们有 Γ_γ 中两对互相交换的对合

$$A = \begin{pmatrix} 0 & I \\ \gamma I & 0 \end{pmatrix},$$

$$B = \begin{pmatrix} 0 & J_1 \\ \gamma J_1 & 0 \end{pmatrix} \quad 及 \quad C = \begin{pmatrix} 0 & J_2 \\ \gamma J_2 & 0 \end{pmatrix},$$

其中 J_1 为 $(1, m-1)$ 对合, 而 J_2 为 $(2, m-2)$ 对合; 可是 AB 为 2 对合而 AC 为 4 对合, 显然, AB 与 AC 在 $PGL_n(K)$ 中不共轭.

定理 4　令 $n = 4$ 而 Γ_γ 为 $PGL_4(K)$ 中第三种对合的集合. 如 -1 为 K 中的平方元素, 则 Γ_γ 中至少有 5 个互相交换的对合; 如果 -1 不是 K 中的平方元素, 则 Γ_γ 中有两对互相交换的对合, 其积在 $PGL_4(K)$ 中不共轭.

【证】 如果 $-1=\lambda^2$, 则我们有 5 个互相交换的对合

$$A_1=\begin{pmatrix}0 & I\\ \gamma I & 0\end{pmatrix},\quad A_2=\begin{pmatrix}0 & \begin{pmatrix}1 & \\ & -1\end{pmatrix}\\ \begin{pmatrix}\gamma & \\ & -\gamma\end{pmatrix} & 0\end{pmatrix},$$

$$A_3=\begin{pmatrix}0 & \begin{pmatrix} & 1\\ 1 & \end{pmatrix}\\ \begin{pmatrix} & \gamma\\ \gamma & \end{pmatrix} & 0\end{pmatrix},\quad A_4=\begin{pmatrix}0 & \begin{pmatrix} & 1\\ -1 & \end{pmatrix}\\ \begin{pmatrix} & -\gamma\\ \gamma & \end{pmatrix} & 0\end{pmatrix},$$

$$A_5=\begin{pmatrix}0 & \begin{pmatrix} & \lambda\\ -\lambda & \end{pmatrix}\\ \begin{pmatrix}0 & \gamma\lambda\\ -\gamma\lambda & 0\end{pmatrix} & 0\end{pmatrix}.$$

如果 $-1=\lambda^2$ 在 K 中不可解, 则 A_1, A_2 与 A_1, A_4 是两对互相交换的对合; 可是

$$A_1A_2=\begin{pmatrix}\gamma & & & \\ & -\gamma & & \\ & & \gamma & \\ & & & -\gamma\end{pmatrix}$$

为 2 对合, 而

$$A_1A_4=\begin{pmatrix}\begin{pmatrix} & -\gamma\\ \gamma & \end{pmatrix} & 0\\ 0 & \begin{pmatrix} & \gamma\\ -\gamma & \end{pmatrix}\end{pmatrix}$$

为 $\Gamma_{-1}(\neq \Gamma_1)$ 中之对合, 因此 A_1A_2 和 A_1A_4 在 $PGL_n(K)$ 中不共轭.

定理 5 设 $n=6$ 而 Γ_γ 为第三种对合的集合, 于是任一 1 对合在 $PGL_6(K)$ 中的中心化子永远不与 Γ_γ 中对合在 $PGL_6(K)$ 中的中心化子同构.

【证】 不失普遍性, 我们可以假定所给 1 对合为

$$A=\begin{pmatrix}1 & 0\\ 0 & -I^{(5)}\end{pmatrix}$$

而所给 Γ_γ 中对合为

$$B=\begin{pmatrix}0 & I^{(3)}\\ \gamma I^{(3)} & 0\end{pmatrix}.$$

将它们在 $PGL_6(K)$ 中之中心化子分别记作 $\mathfrak{Z}_A$ 和 $\mathfrak{Z}_B$.

$\mathfrak{Z}_A$ 为由所有元素 $\overline{R}$ 适合 $RA = AR$ 或 $RA = -AR$ 者所组成, 可是这时 $RA = -AR$ 不可能发生, 因为否则 R 将交换 A 的加空间和减空间, 而这两空间的维数不等. 由 $RA = AR$ 可推知

$$R = \begin{pmatrix} \eta & 0 \\ 0 & R^{(5)} \end{pmatrix},$$

于是 $\mathfrak{Z}_A$ 与 $GL_1(K) \times GL_5(K)$ 对其中心的商群同构. 写

$$\mathfrak{Z}_A \cong K^*/Z^* \times PGL_5(K).$$

我们知道 (定理 3.1), $PSL_5(K)$ 为单群, 因之 $\mathfrak{Z}_A$ 有正规群列

$$\mathfrak{Z}_A \supset PGL_5(K) \supset PSL_5(K) \supset \mathfrak{E}$$

($\mathfrak{E}$ 表示仅由单位矩阵组成的群), 其中一个商群与单群 $PSL_5(K)$ 同构.

$\mathfrak{Z}_B$ 由所有元素 $\overline{R}$, 而 $RB = BR$ 或 $RB = -BR$ 所组成, 这时, 第二个关系是可能的, 例如我们可以取

$$R = \begin{pmatrix} 0 & I \\ -\gamma I & 0 \end{pmatrix},$$

可是元素 $\overline{R}$ 使 $RB = BR$ 者组成 $\mathfrak{Z}_B$ 的一个指数 2 的子群 $\mathfrak{Z}'_B$, 因为由 $RB = -BR$ 及 $TB = -BT$ 可推出 $(RT)B = B(RT)$. 我们来研究 $\mathfrak{Z}'_B$. 关系 $RB = BR$ 成立当且仅当

$$R = \begin{pmatrix} R_1^{(3)} & R_2^{(3)} \\ \gamma R_2^{(3)} & R_1^{(3)} \end{pmatrix}.$$

显然, 所有这种元素组成一群 Z'_B. 以 K_0 表示由 K 经添加一个中心元素 ω 适合 $\gamma = \omega^2$ 者到 K 而得到的体, 则易见

$$\begin{pmatrix} R_1 & R_2 \\ \gamma R_2 & R_1 \end{pmatrix} \to R_1 + \omega R_2$$

为由 Z'_B 到 $GL_3(K_0)$ 之上的一个同构映射, 于是

$$\mathfrak{Z}'_B \cong PGL_3(K_0).$$

因此 $\mathfrak{Z}_B$ 有正规群列

$$\mathfrak{Z}_B \supset \mathfrak{Z}'_B(\cong PGL_3(K_0)) \supset PSL_3(K_0) \supset \mathfrak{E},$$

其中所有商群除去一个是单群 $PSL_3(K_0)$ 外都是 Abel 群.

现在我们来证明 $\mathfrak{Z}_A$ 与 $\mathfrak{Z}_B$ 不同构. 如果它们同构, 则由 Jordan-Hölder-Schreier 定理, 在 $\mathfrak{Z}_A$ 的组合群列的商群中出现的非 Abel 单群 $PSL_5(K)$ 必与在 $\mathfrak{Z}_B$ 的组合群列的商群中出现的唯一的非 Abel 单群 $PSL_3(K_0)$ 同构. 因此只要证明 $PSL_5(K)$ 与 $PSL_3(K_0)$ 不同构就行了. 在 $PGL_3(K_0)$ 中, 互相交换的 1 对合的最大个数为 3, 而这些对合因为对应于 $GL_3(K_0)$ 中的 (1, 2) 对合, 所以属于 $PSL_3(K_0)$. 可是在 $PSL_5(K)$ 中, 依定理 1 之系理, 互相交换的 r 对合的最小个数为 5, 而仿定理 2 的系理 2, 易证 $PSL_5(K)$ 中互相交换的在 $PSL_5(K)$ 之中共轭的第二种对合的个数 $\geqslant 2^4 = 16$. 因之, $PSL_3(K_0)$ 决不与 $PSL_5(K)$ 同构, 定理证毕.

在本节中我们已经把 $PGL_n(K)$ 中的 1 对合用群论性质刻画了出来. 换言之, 我们把 $PGL_n(K)$ 中的 1 对合用在 $PGL_n(K)$ 的自同构之下不变的性质从其他种对合里区分出来, 这结果能够用来决定 $PGL_n(K)$ 的自同构群, 可是对于 $PSL_n(K)$ 而言, 我们还需要作更进一步的探讨.

§7 $PGL_n(K), PSL_n^{\pm}(K)$ 和 $PSL_n(K)$ 的自同构 (特征数 $\neq 2$)

像在 §5 中一样, 我们先来决定 $PSL_n(K)$ 的自同构, 然后再推出 $PGL_n(K)$ 和 $PSL_n^{\pm}(K)$ 的结果来, 当然, 我们假定 $n \geqslant 3$.

定理 1 设 $n \geqslant 3$, 则 $PSL_n(K)$ 的自同构皆由 $SL_n(K)$ 的自同构诱导出来, 或者, 确切地说, 它的形状是

(1) $$\overline{A} \to \overline{P}\,\overline{A^\sigma}\,\overline{P}^{-1},$$

其中 σ 为体 K 之自同构, 而 P 为可逆矩阵; 或者是

(2) $$\overline{A} \to \overline{P}(\overline{A^\tau})'^{-1}\overline{P}^{-1},$$

其中 τ 为 K 之反自同构.

这个定理的证明依赖于以下诸引理.

引理 1 任意集 Γ_γ 中, 任意两个不同的互相交换的对合之积属于 Γ_1 或 Γ_{-1}.

【证】 设 $A^2 = B^2 = \gamma I, A \neq \pm B, AB = \pm BA$, 则有

$$(AB)^2 = \pm A^2B^2 = \pm\gamma^2 I.$$

即 $AB \in \Gamma_1$ 或 Γ_{-1}.

引理 2 设 $n = 2m \geqslant 8$, 则 $PSL_n(K)$ 中互相交换的 2 对合的最大数小于互相交换的 m 对合的最大数.

【证】 因 $n \geqslant 8$, 故 $m \geqslant 4$. 于是

$$\frac{1}{2}\begin{pmatrix} 2m \\ m \end{pmatrix} \geqslant \frac{1}{2}\begin{pmatrix} 2m \\ 4 \end{pmatrix} = \frac{1}{2}\frac{2m(2m-1)(2m-2)(2m-3)}{1\cdot 2\cdot 3\cdot 4} > \begin{pmatrix} 2m \\ 2 \end{pmatrix}.$$

因此引理得证.

引理 3 设 Γ_{-1} 为 $PSL_n(K)$ 中数量为 -1 的第二种对合的集合, 则 Γ_{-1} 中任意在 $PSL_n(K)$ 之下共轭的共轭元素类中至少有 2^{n-1} 个或 2^{n-2} 个互相交换的对合, 依 n 为奇或偶而定.

【证】 依定理 6.2, 只要证 Γ_{-1} 中含

$$[\lambda, \lambda, \cdots, \lambda]$$

的共轭元素类有此性质即可. 令 $T = [t_1, t_2, \cdots, t_n]$ 为对角矩阵, 其中 $t_i = \xi, \xi^{-1}$ 或 1, 使得 t_i 取 ξ 的个数等于 t_i 取 ξ^{-1} 的个数 ($\xi = \lambda\mu - \mu\lambda \neq 0$). 则当 T 跑过所有可能性时,

$$T[\lambda, \lambda, \cdots, \lambda]T^{-1}$$

就给我们 2^{n-1} 或 $\frac{1}{2}2^{n-1} = 2^{n-2}$ 个互相交换而且互相共轭的对合, 依 n 为奇或偶而定.

定理 2 设 Γ_{-1} 为 $PSL_n(K)$ 中具数量 -1 的第二种对合的集合, 则 Γ_{-1} 中任一对合在 $PSL_n(K)$ 中之中心化子永远不和 2 对合在 $PSL_n(K)$ 中之中心化子同构 (当然 $n \geqslant 4$).

【证】 不失普遍性, 可以取

$$A = [\lambda, \lambda, \cdots, \lambda], \quad B = \begin{pmatrix} -I^{(2)} & 0 \\ 0 & I^{(n-2)} \end{pmatrix}$$

分别作为 Γ_{-1} 中的对合和 2 对合, 以 $\overline{\mathfrak{Z}}_A$ 与 $\overline{\mathfrak{Z}}_B$ 分别表它们在 $PSL_n(K)$ 中之中心化子.

$\overline{\mathfrak{Z}}_A$ 由元素 $\overline{R}$ 而适合 $RA = AR$ 或 $RA = -AR$ 者所组成. 如果 $RA = -AR$ 可能成立, 则 $\overline{\mathfrak{Z}}_A$ 中元素 $\overline{R}$ 适合 $RA = AR$ 者组成一指数 2 的正规子群 $\overline{\mathfrak{Z}}'_A$. 如果 $RA = -AR$ 不可能成立, 我们定义 $\overline{\mathfrak{Z}}'_A = \overline{\mathfrak{Z}}_A$. 现在我们来研究 $\overline{\mathfrak{Z}}'_A$. 将体 K 之乘法群之中心记作 Z^*, 则

$$\overline{\mathfrak{Z}}'_A \cong SL_n(K_\lambda)/Z_k^* I^{(n)},$$

其中 K_λ 表 λ 在 K 中之中心化子. 因此 $\overline{\mathfrak{Z}}_A$ 有正规群列

$$\overline{\mathfrak{Z}}_A \supset \overline{\mathfrak{Z}}'_A \cong SL_n(K_\lambda)/Z_k^* I^{(n)} \supset Z_{K_\lambda}^* I^{(n)}/Z^* I^{(n)} \supset \mathfrak{E}$$

($Z_{K_\lambda}^*$ 表 K_λ 的中心的乘法群), 其中所有商群都是 Abel 群, 除去一个例外:

$$\frac{SL_n(K_\lambda)/Z_k^* I^{(n)}}{Z_{K_\lambda}^* I^{(n)}/Z^* I^{(n)}} \cong SL_n(K_\lambda)/Z_{K_\lambda}^*/I^{(n)} = PSL_n(K_\lambda).$$

现在来研究 $\mathfrak{Z}_B$. $\mathfrak{Z}_B$ 由元素 $\overline{R}$ 适合 $RB = BR$ 或 $RB = -BR$ 者组成. 如 $n \neq 4$, 第二个关系不可能成立, 而当 $n = 4$ 时, 取

$$R = \begin{pmatrix} 0 & I^{(2)} \\ I^{(2)} & 0 \end{pmatrix},$$

则 $RB = -BR$, 这时 $\mathfrak{Z}_B$ 中元素 $\overline{R}$ 适合 $RB = BR$ 者组成一指数 2 的正规子群 $\mathfrak{Z}_B'$. 如 $n \neq 4$, 令 $\mathfrak{Z}_B' = \mathfrak{Z}_B$. 我们来研究 $\mathfrak{Z}_B'$. 显然 $\mathfrak{Z}_B'$ 由 $\overline{R}$ 所组成, 而

$$R = \begin{pmatrix} R^{(2)} & 0 \\ 0 & R^{(n-2)} \end{pmatrix},$$

其中 $R^{(2)}$ 和 $R^{(n-2)}$ 分别跑过 $GL_2(K)$ 和 $GL_{n-2}(K)$ 而

$$\det(R^{(2)})\det(R^{(n-2)}) = 1.$$

因之 $\mathfrak{Z}_B'$ 的换位子群包有 $PSL_2(K) \times PSL_{n-2}(K)$. 于是 $\mathfrak{Z}_B$ 有正规群列

$$\mathfrak{Z}_B \supset \mathfrak{Z}_B' \supset PSL_2(K) \times PSL_{n-2}(K) \supseteq PSL_2(K) \supseteq \mathfrak{E},$$

其中有两个商群 $PSL_2(K)$ 和 $PSL_{n-2}(K)$ 是非 Abel 单群.

依 Jordan-Hölder-Schreier 定理, $\mathfrak{Z}_A$ 和 $\mathfrak{Z}_B$ 不同构.

定理 3 设 Γ_{-1} 为 $PSL_n(K)$ 中具数量 -1 的第三种对合的集合, 则 Γ_{-1} 中任一元素在 $PSL_n(K)$ 中之中心化子不与 2 对合在 $PSL_n(K)$ 中之中心化子同构 (当然, $n \geqslant 4$).

【证】 不失普遍性, 可以取

$$A = \begin{pmatrix} 0 & I^{(m)} \\ -I^{(m)} & 0 \end{pmatrix}, \quad B = \begin{pmatrix} -I^{(2)} & 0 \\ 0 & I^{(n-2)} \end{pmatrix},$$

其中 $m = \dfrac{n}{2}$, 将它们在 $PSL_n(K)$ 中之中心化子分别记作 $\mathfrak{Z}_A$ 和 $\mathfrak{Z}_B$.

$\mathfrak{Z}_A$ 由 $PSL_n(K)$ 中元素 $\overline{R}$ 适合 $RA = AR$ 或 $RA = -AR$ 者所组成, 记 $\mathfrak{Z}_A'$ 为 $PSL_n(K)$ 中元素 $\overline{R}$ 适合 $RA = AR$ 者所组成之子群, 则 $\mathfrak{Z}_A'$ 为 $\mathfrak{Z}_A$ 之指数 2 的正规子群或 $\mathfrak{Z}_A' = \mathfrak{Z}_A$. 我们来研究 $\mathfrak{Z}_A'$. 关系 $RA = AR$ 成立, 当且仅当

$$R = \begin{pmatrix} R_1^{(m)} & R_2^{(m)} \\ -R_2^{(m)} & R_1^{(m)} \end{pmatrix}.$$

显然, 所有这种元素其行列式 $\neq 0$ 者组成一群 $\mathfrak{Z}'_A$, 而

$$\overline{\mathfrak{Z}}'_A \cong \mathfrak{Z}'_A / Z^* I^{(n)} \cap SL_n(K).$$

以 K_0 表添加一个中心元素 ω 适合 $-1 = \omega^2$ 到 K 而得到的体, 则映射

$$\begin{pmatrix} R_1 & R_2 \\ -R_2 & R_1 \end{pmatrix} \rightarrow R_1 + \omega R_2$$

为从 $\mathfrak{Z}'_A$ 映入 $GL_m(K_0)$ 之同构映射, 而且 $\mathfrak{Z}'_A$ 之映像包有 $SL_m(K_0)$. 因此 $\overline{\mathfrak{Z}}_A$ 有正规群列, 其中只有一个商群不是 Abel 群, 而是单群 $PSL_m(K_0)$. (注意 K_0 至少含 $9 = 3^2$ 个元素).

在定理 2 中已证明 $\overline{\mathfrak{Z}}_B$ 有正规群列

$$\overline{\mathfrak{Z}}_B \supset \overline{\mathfrak{Z}}'_B \supset PSL_2(K) \times PSL_{n-2}(K) \supset PSL_2(K) \supset \mathfrak{E},$$

其中有两个商群是 $PSL_2(K)$ 和 $PSL_{n-2}(K)$, 而其余的商群都是 Abel 群. 如 K 含 3 元以上, 则 $PSL_2(K)$ 和 $PSL_{n-2}(K)$ 都是单群, 依 Jordan-Hölder-Schreier 定理, $\overline{\mathfrak{Z}}_A$ 和 $\overline{\mathfrak{Z}}_B$ 不能同构. 如 K 只有 3 元, 而 $n = 4$, 则 $PSL_2(K)$ 和 $PSL_{n-2}(K)$ 都不是单群, 因之依同一定理, $\overline{\mathfrak{Z}}_A$ 和 $\overline{\mathfrak{Z}}_B$ 也不同构. 最后, 如果 K 只有 3 元, 而 $n \geqslant 6$, 则 $PSL_{n-2}(K)$ 是单群, 而 $PSL_2(K)$ 不是单群, 可是 $PSL_{n-2}(F_3) : 1 \neq PSL_m(F_9) : 1$, 因此依同一定理, $\overline{\mathfrak{Z}}_A$ 和 $\overline{\mathfrak{Z}}_B$ 不同构. 证毕.

现在我们来证明定理 1. 我们对 n 用归纳法.

(i)$n = 3$. 首先, 我们知道 1 对合是属于 $PSL_3(K)$ 的, 我们要证明 $PSL_3(K)$ 的自同构将 1 对合变到 1 对合. 因

$$[-1, -1, 1] \quad \text{和} \quad [1, -1, -1]$$

是两个不同的互相交换的 1 对合, 而其积仍为 1 对合, 故依引理 1 知 1 对合只能变到 Γ_1 或 Γ_{-1} 中之对合, 现在 Γ_1 仅由 1 对合组成, 而第三种对合不在 $PSL_3(K)$ 中出现, 所以只要能证 1 对合不能变到 Γ_1 中的第二种对合就行了. 因为互相交换的 1 对合的最大个数是 3 而 Γ_{-1} 中互相交换且互相共轭的第二种对合的个数 $> 2^2 = 4$, 因之, $PSL_3(K)$ 的自同构将 1 对合变到 1 对合.

像定理 5.1(I) 一样进行下去, 即得本定理.

(ii)$n \geqslant 4$. 这时 2 对合属于 $PSL_n(K)$. 因为

$$[-1, -1, 1, 1, \cdots, 1] \quad \text{和} \quad [-1, 1, -1, 1, \cdots, 1]$$

是两个不同的互相交换的 2 对合, 而其积为 2 对合, 故依引理 1 知 $PSL_n(K)$ 的自同构只能将 2 对合变到 Γ_1 或 Γ_{-1} 中的对合. 依定理 2 和 3 知 $PSL_n(K)$ 的自同构

不能把 2 对合变到 Γ_{-1} 中的对合, 如 $\Gamma_{-1} \neq \Gamma_1$. 还要证明 $PSL_n(K)$ 的自同构不能把 r 对合变到 2 对合, 如 $r \neq 2$. 我们分以下几个情形来研究:

1°　$n > 4, r \neq \frac{n}{2}$. 这可由定理 6.1 推出上述断言.

2°　$n \geqslant 8$ 为偶且 $r = \frac{n}{2}$. 这可由引理 2 推得.

3°　$n = 6, r = 3$. 因任意两个不同的互相交换的 2 对合之积仍为 2 对合, 而两个不同的互相交换的 3 对合之积不是 3 对合, 故断言也成立.

4°　$n = 4$, 而 1 对合不属于 $PSL_4(K)$, 这时 2 对合是 $PSL_4(K)$ 中仅有的 r 对合, 断言当然成立.

5°　$n = 4$, 而 1 对合属于 $PSL_4(K)$, 这时断言可以从系理 6.2 推出.

因此我们证明了 $PSL_n(K)$ 的自同构一定将 2 对合变到 2 对合. 我们可以像定理 5.1 一样进行下去, 从而证明本定理. (需要指出, 如 $n = 4$, 则 $PSL_4(K)$ 中与 $[-1,-1,1,1]$ 交换的元素的形状是 $\begin{pmatrix} A & 0 \\ 0 & B \end{pmatrix}$ 或 $\begin{pmatrix} 0 & C \\ D & 0 \end{pmatrix}$, 将这些元素平方之后, 即可像定理 5.1 那样进行下去.)

定理 1 的直接推论是

定理 4　设 $n \geqslant 3$, $PGL_n(K)$(或 $PSL_n^{\pm}(K)$) 的自同构系由 $GL_n(K)$(或 $SL_n^{\pm}(K)$) 的自同构所诱导出来的, 或者说, 它的形状是定理 1 中的 (1) 或 (2).

§8　对合 (特征数 = 2)

$GL_n(K)$ 及 $SL_n(K)$ 的自同构的研究 (K 为特征数 = 2 的体), 仍依赖于对合的研究. 在 §8 ~ §9 中我们恒假定 K 的特征数 = 2.

定理 1　$GL_n(K)$ 中之对合在 $GL_n(K)$ 之下相似于

$$(1)\qquad \begin{pmatrix} 1 & 1 \\ & 1 \end{pmatrix} \dotplus \begin{pmatrix} 1 & 1 \\ & 1 \end{pmatrix} \dotplus \cdots \dotplus \begin{pmatrix} 1 & 1 \\ & 1 \end{pmatrix} \dotplus 1 \dotplus 1 \dotplus \cdots \dotplus 1,$$

而且也相似于

$$(2)\qquad \begin{pmatrix} I^{(p)} & I^{(p)} & 0 \\ 0 & I^{(p)} & 0 \\ 0 & 0 & I^{(n-2p)} \end{pmatrix},$$

其中 p 为 (1) 式中 $\begin{pmatrix} 1 & 1 \\ & 1 \end{pmatrix}$ 的个数.

【证】　令 A 为 $GL_n(K)$ 之对合, 由 $A^2 = I$ 推出 $(A-I)^2 = 0$. 设 $A - I$ 的秩为 p, 则有 $n \times n$ 可逆矩阵 P 存在, 使

$$P(A-I)P^{-1} = \begin{pmatrix} B_1^{(p)} & B_2^{(p,n-p)} \\ 0 & 0 \end{pmatrix},$$

其中 (B_1, B_2) 的秩为 p. 因 $(A-I)^2=0$, 故

$$B_1(B_1 \quad B_2)=0,$$

于是 $B_1=0$. 因之 B_2 的秩为 p. 由此推出 $p \leqslant n-p$. 设 Q 为 $(n-p)\times(n-p)$ 可逆矩阵, 使

$$B_2Q=(I^{(p)} \quad 0),$$

则

$$\begin{pmatrix} I & \\ & Q^{-1} \end{pmatrix} P(A-I)P^{-1} \begin{pmatrix} I & \\ & Q^{-1} \end{pmatrix}^{-1} = \begin{pmatrix} 0^{(p)} & I^{(p)} & 0 \\ & & 0 \end{pmatrix},$$

于是 A 与 (2) 相似.

由此定理推知 $GL_n(K)$ 中之对合都属于 $SL_n(K)$.

定义 1　$GL_n(K)$ 或 $SL_n(K)$ 中之对合在 $GL_n(K)$ 之下相似于 (2) 者称为 p 对合.

显然, 我们只有 p 对合而 $2p \leqslant n$, 而且, p 对合在 $SL_n(K)$ 之下永远相似于 (2), 除非 $2p=n$.

定理 2　p 对合在 $GL_n(K)$ 之下相似于 q 对合, 当且仅当 $p=q$. 如 $2p<n$, 则任意两 p 对合在 $SL_n(K)$ 之下皆相似; 如 $2p=n$, 则有 p 对合在 $SL_n(K)$ 之下不相似者.

【证】　将 p 对合看作作用在 V_n 上的一个线性变换, 则其不变子空间为 V_n 的一个 $n-p$ 维的子空间, 因此 p 对合与 q 对合在 $GL_n(K)$ 之下相似, 当且仅当 $p=q$.

第二个断言显然成立.

为要证第三个断言, 我们注意 $GL_{2p}(K)$ 中与

$$\begin{pmatrix} I^{(p)} & I^{(p)} \\ 0 & I^{(p)} \end{pmatrix} \tag{3}$$

交换的矩阵的形状为

$$\begin{pmatrix} A & B \\ 0 & A \end{pmatrix},$$

其中 A 可逆, 因此它们的行列式为 K^*/C 中之平方元素, 所以用 K^*/C 中一个具非平方元素行列式的矩阵来变 (3) 就得到一个不与 (3) 在 $SL_{2p}(K)$ 之下共轭的 p 对合.

定理 3　$GL_n(K)$ 中的对合分到了 $\left[\frac{n}{2}\right]$ 个共轭 p 对合类里, $1 \leqslant p \leqslant \left[\frac{n}{2}\right]$. $p \neq \frac{n}{2}$ 的 p 对合类仍是 $SL_n(K)$ 中的一个共轭类. 可是如果 $p=\frac{n}{2}$, 则 $GL_n(K)$ 中的 p 对合类可以由 $SL_n(K)$ 中一个以上的共轭类组成.

我们的目的是要将 $SL_n(K)$ 中的 1 对合刻画出来. 如果 $n=2$ 或 3, 则我们只有 1 对合, 因之我们无事可做. 若 $n \geqslant 6$, 我们有

定理 4 设 $n \geqslant 6$. 任意两个互相交换的 1 对合的乘积落在不多于两个共轭对合类里. 任意两个互相交换而且在 $SL_n(K)$ 之下共轭的 p 对合 $(p \geqslant 2)$ 的乘积落在多于两个共轭对合类里.

【证】 令 $A=I+U, B=I+V$ 为两个互相交换的对合, 即 $U^2=V^2=0, UV=VU$. 它们的乘积

$$AB=BA=I+U+V+UV$$

也为对合, 因为 $(U+V+UV)^2=0$.

如果 A 和 B 为两个 1 对合, 则 U 和 V 的秩为 1, 于是

$$U+(I+U)V$$

之秩 $\leqslant 2$, 这就是说, AB 或为 1 对合或为 2 对合.

如 $p>1$, 我们取

$$U=\begin{pmatrix} 0^{(p)} & U_1^{(p)} & 0 \\ 0 & 0^{(p)} & 0 \\ 0 & 0 & 0^{(n-2p)} \end{pmatrix},$$
$$V=\begin{pmatrix} 0^{(p)} & V_1^{(p)} & 0 \\ 0 & 0^{(p)} & 0 \\ 0 & 0 & 0^{(n-2p)} \end{pmatrix},$$

其中

$$U_1^{(p)}=I_1^{(p)}, V_1^{(p)}=\begin{pmatrix} 1 & & & & & \\ & 1 & \overbrace{1 \quad \ddots \quad 1}^{q\text{个}} & & & \\ & & 1 & \ddots & & \\ & & & \ddots & 1 & \\ & & & & \ddots & 1 \\ & & & & & 1 \end{pmatrix},$$

则 A, B 为交换 p 对合 (如 $n=2p$, 它们在 $SL_n(K)$ 中也共轭). 因为

$$U_1^{(p)}+V_1^{(p)}=\begin{pmatrix} 0 & & & & & \\ & 0 & 1 & & q\text{个} & \\ & & 0 & \ddots & & \\ & & & \ddots & 1 & \\ & & & & \ddots & 1 \\ & & & & & 0 \end{pmatrix},$$

所以 AB 为 q 对合. 取 $q=1,2,\cdots,p-1$, 我们知道两个互相交换的 p 对合之积落在 $p-1$ 个共轭类里, 因此, 如果 $p>3$, 定理得证.

如 $p=3$, 再取

$$U_1^{(3)}=I^{(3)}, V_1^{(3)}=\begin{pmatrix} 0 & 0 & 1 \\ 1 & 1 & 0 \\ 0 & 1 & 1 \end{pmatrix},$$

则

$$U_1+V_1=\begin{pmatrix} 1 & 0 & 1 \\ 1 & 0 & 0 \\ 0 & 1 & 0 \end{pmatrix},$$

所以 AB 为 3 对合, 因之这时我们的定理得证.

如 $p=2$, 取

$$U_1^{(2)}=I^{(2)}, \quad V_1^{(2)}=\begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix},$$

则 AB 为 2 对合. 如再取

$$A=\begin{pmatrix} 1 & & & 0 & 0 & 1 & \\ & 1 & & 0 & 1 & 0 & \\ & & 1 & 0 & 1 & 1 & \\ & & & 1 & & & \\ & & & & 1 & & \\ & & & & & 1 & \\ & & & & & & I \end{pmatrix}, \quad B=\begin{pmatrix} 1 & & & 1 & 0 & 0 & \\ & 1 & & 0 & 0 & 0 & \\ & & 1 & 0 & 1 & 0 & \\ & & & 1 & & & \\ & & & & 1 & & \\ & & & & & 1 & \\ & & & & & & I \end{pmatrix},$$

则 AB 为 3 对合. 定理至此完全证毕.

当 $n=4$ 及 $n=5$ 时我们如下地进行.

定理 5 设 $n\geqslant 3$, 在 $SL_n(K)$ 中任意一对 1 对合, 如其积之阶为 3, 则可同时化成

(4)
$$\begin{pmatrix} 1 & 1 & \\ 0 & 1 & 0 \\ 0 & & I^{(n-2)} \end{pmatrix},\quad \begin{pmatrix} 1 & 0 & \\ 1 & 1 & 0 \\ 0 & & I^{(n-2)} \end{pmatrix}.$$

【证】 令 $A = I + U$ 和 $B = I + V$ 为一对 1 对合而 AB 之阶为 3, 则 $U^2 = V^2 = 0$ 而 U 和 V 之秩为 1. 由

$$ABA = BAB,$$

即

$$(I+U)(I+V)(I+U) = (I+V)(I+U)(I+V)$$

可得

(5)
$$U + V + UVU + VUV = 0.$$

将 (5) 左乘以 U 则得

$$(UV)^2 = UV,$$

也有

$$(VU)^2 = VU.$$

假定 U 已化成了

$$U = \begin{pmatrix} 0 & 1 & 0 \\ 0 & 0 & 0 \\ 0 & 0 & 0 \end{pmatrix}.$$

则

$$V = \begin{pmatrix} a & b & p \\ c & d & q \\ r & t & u \end{pmatrix},$$

其中 $a, b, c, d \in K, p, q$ 为 $1 \times (n-2)$ 矩阵, r, t 为 $(n-2) \times 1$ 矩阵, u 为 $(n-2) \times (n-2)$ 矩阵. 若 $c = 0, r = 0$, 则因 $V^2 = 0$, 必有 $a = 2$. 若 $c \neq 0$ 或 $r \neq 0$, 则

$$\begin{pmatrix} 1 & \lambda & \mu \\ & 1 & \\ & & I \end{pmatrix}\begin{pmatrix} 0 & 1 & 0 \\ 0 & 0 & 0 \\ 0 & 0 & 0 \end{pmatrix}\begin{pmatrix} 1 & \lambda & \mu \\ & 1 & \\ & & I \end{pmatrix}^{-1} = \begin{pmatrix} 0 & 1 & 0 \\ 0 & 0 & 0 \\ 0 & 0 & 0 \end{pmatrix},$$

$$\begin{pmatrix} 1 & \lambda & \mu \\ & 1 & \\ & & I \end{pmatrix}\begin{pmatrix} a & b & p \\ c & d & q \\ r & t & u \end{pmatrix}\begin{pmatrix} 1 & \lambda & \mu \\ & 1 & \\ & & I \end{pmatrix}^{-1} = \begin{pmatrix} a + \lambda c + \mu r & \\ c & * \\ r & \end{pmatrix}.$$

可选取 λ, μ, 使 $a+\lambda c+\mu r=0$, 因之我们总可假定 $a=0$, 即

$$V=\begin{pmatrix}0&b&p\\c&d&q\\r&t&u\end{pmatrix}.$$

我们有

$$VU=\begin{pmatrix}0&0&0\\0&c&0\\0&r&0\end{pmatrix},\quad (VU)^2=\begin{pmatrix}0&0&0\\0&c^2&0\\0&rc&0\end{pmatrix},$$

因此 $c^2=c$. 所以 $c=0$ 或 $c=1$.

首先我们证明 $c=0$ 是不可能的. 因为如果 $c=0$, 则 $r=0$, 于是

$$V=\begin{pmatrix}0&b&p\\0&d&q\\0&t&u\end{pmatrix},\quad UV=\begin{pmatrix}0&d&q\\0&0&0\\0&0&0\end{pmatrix},\quad (UV)^2=0,$$

因此 $d=0, q=0$. 这就是

$$V=\begin{pmatrix}0&b&p\\0&0&0\\0&t&u\end{pmatrix},$$

于是 $UV=VU$. 这是不可能的.

因此, 我们一定有 $c=1$. 因为 V 的秩为 1, 故

$$V=\begin{pmatrix}0&0&0\\1&d&p\\r&t&u\end{pmatrix},$$

因为

$$\begin{pmatrix}1&&\\&1&\\&r&I\end{pmatrix}\begin{pmatrix}0&1&0\\0&0&0\\0&0&0\end{pmatrix}\begin{pmatrix}1&&\\&1&\\&r&I\end{pmatrix}^{-1}=\begin{pmatrix}0&1&0\\0&0&0\\0&0&0\end{pmatrix},$$
$$\begin{pmatrix}1&&\\&1&\\&r&I\end{pmatrix}\begin{pmatrix}0&0&0\\1&d&q\\r&t&u\end{pmatrix}\begin{pmatrix}1&&\\&1&\\&r&I\end{pmatrix}^{-1}=\begin{pmatrix}0&0&0\\1&*&*\\0&*&*\end{pmatrix},$$

所以我们可以假定 $r=0$. 于是 $t=0, u=0$, 那么

$$V=\begin{pmatrix}0&0&0\\1&d&q\\0&0&0\end{pmatrix},\quad V^2=\begin{pmatrix}0&0&0\\d&d^2&dq\\0&0&0\end{pmatrix}.$$

由 $V^2=0$ 推出 $d=0$. 最后,

$$\begin{pmatrix}1&&q\\&1&\\&&I\end{pmatrix}\begin{pmatrix}0&1&0\\0&0&0\\0&0&0\end{pmatrix}\begin{pmatrix}1&&q\\&1&\\&&I\end{pmatrix}^{-1}=\begin{pmatrix}0&1&0\\0&0&0\\0&0&0\end{pmatrix},$$

$$\begin{pmatrix}1&&q\\&1&\\&&I\end{pmatrix}\begin{pmatrix}0&0&0\\1&0&q\\0&0&0\end{pmatrix}\begin{pmatrix}1&&q\\&1&\\&&I\end{pmatrix}^{-1}=\begin{pmatrix}0&0&0\\1&0&0\\0&0&0\end{pmatrix},$$

所以

$$V=\begin{pmatrix}0&0&0\\1&0&0\\0&0&0\end{pmatrix}.$$

定理证毕.

定理 6 设 $n=5$ 或 $n=4$ 而 $K\neq F_2$.$SL_n(K)$ 中 1 对合之对 (4) 在 $SL_n(K)$ 中的中心化子永不与 2 对合之对

$$\begin{pmatrix}I^{(2)}&I^{(2)}&\\&I^{(2)}&\\&&I^{(n-4)}\end{pmatrix} \text{和} \begin{pmatrix}I^{(2)}&&\\I^{(2)}&I^{(2)}&\\&&I^{(n-4)}\end{pmatrix} \tag{6}$$

在 $SL_n(K)$ 中的中心化子同构.

【证】 (4) 和 (6) 的中心化子分别记作 $\mathfrak{Z}_1$ 和 $\mathfrak{Z}_2$. 则 $\mathfrak{Z}_1$ 由形如

$$\begin{pmatrix}a&&\\&a&\\&&A^{(n-2)}\end{pmatrix}$$

的元素组成, 其中 $\varphi(a)^2\det A=1$; 而 $\mathfrak{Z}_2$ 由形如

$$\begin{pmatrix}B^{(2)}&&\\&B^{(2)}&\\&&C^{(n-4)}\end{pmatrix}$$

的元素组成, 其中 $(\det B)^2\cdot\det C=1$. 区别以下两种情形.

(i)$n=5$. 以 $\mathfrak{Z}_1^*$ 和 $\mathfrak{Z}_2^*$ 表 $\mathfrak{Z}_1$ 和 $\mathfrak{Z}_2$ 中对合所生成的子群, 则 $\mathfrak{Z}_1^*$ 由形如

$$\begin{pmatrix} 1 & & \\ & 1 & \\ & & A \end{pmatrix}$$

的元素组成, 其中 $A \in SL_3(K)$; 而 $\mathfrak{Z}_2^*$ 由形如

$$\begin{pmatrix} B & & \\ & B & \\ & & 1 \end{pmatrix}$$

的元素组成, 其中 $B \in SL_2(K)$. 于是

$$\mathfrak{Z}_1^* \cong SL_3(K), \quad \mathfrak{Z}_2^* \cong SL_2(K).$$

可是 $SL_3(K)$ 中与一个 1 对合交换的 1 对合的全体组成一个不可换集, 而 $SL_2(K)$ 中与一个 1 对合交换的 1 对合的全体组成一个可换集, 因此 $SL_3(K) \ncong SL_2(K)$. 因之, $\mathfrak{Z}_1 \ncong \mathfrak{Z}_2$.

(ii)$n=4$. 这时 $\mathfrak{Z}_1$ 由形如

$$\begin{pmatrix} a & & \\ & a & \\ & & A^{(2)} \end{pmatrix} \tag{7}$$

的元素组成, 其中 $\varphi(a)^2 \det A = 1$; 而 $\mathfrak{Z}_2$ 由形如

$$\begin{pmatrix} B^{(2)} & \\ & B^{(2)} \end{pmatrix}$$

的元素组成, 其中 $(\det B)^2 = 1$. 如 K 为域, 这时由 $(\det B)^2 = 1$ 推出 $\det B = 1$; 于是, 如 $K \neq F_2$, 则 $\mathfrak{Z}_1$ 中形如 (7) 的元素而 $a=1$ 者组成 $\mathfrak{Z}_1$ 的一个真非中心正规子群, 但是 $\mathfrak{Z}_2 \cong SL_2(K)$ 没有真非中心正规子群, 因之 $\mathfrak{Z}_1 \ncong \mathfrak{Z}_2$.

如 K 不是域, 设 $\mathfrak{Z}_1$ 和 $\mathfrak{Z}_2$ 同构, 则 $\mathfrak{Z}_1$ 的换位子群 $\mathfrak{Z}_1'$ 和 $\mathfrak{Z}_2$ 的换位子群 $\mathfrak{Z}_2'$ 同构. 同上可证 $\mathfrak{Z}_1'$ 有真非中心正规子群而 $\mathfrak{Z}_2'$ 没有, 因之 $\mathfrak{Z}_1 \ncong \mathfrak{Z}_2$.

定理 7　设 $n \geqslant 4, SL_n(K)$ 的自同构必将 1 对合映到 1 对合.

【证】　如 $n \geqslant 6$, 本定理是定理 4 的直接推论, 以下设 $n=4$ 或 5.

如 $n=4$, 而 K 只有二元, 计算一下, 1 对合及 2 对合在 $SL_4(K)$ 中的中心化子之阶即可证明 1 对合不可能映到 2 对合.

设 $n=5$ 或 $n=4$ 而 $K\neq F_2$. 假定 $SL_n(K)$ 中有 1 对合映到了 2 对合, 不妨假定

$$\begin{pmatrix} 1 & 1 & \\ & 1 & \\ & & I \end{pmatrix} \to \begin{pmatrix} I^{(2)} & I^{(2)} & \\ & I^{(2)} & \\ & & I^{(n-4)} \end{pmatrix}.$$

考虑映到 2 对合

$$\begin{pmatrix} I^{(2)} & & \\ I^{(2)} & I^{(2)} & \\ & & I^{(n-4)} \end{pmatrix}$$

的 1 对合, 依定理 5 可设

$$\begin{pmatrix} 1 & & \\ 1 & 1 & \\ & & I \end{pmatrix} \to \begin{pmatrix} I^{(2)} & & \\ I^{(2)} & I^{(2)} & \\ & & I^{(n-4)} \end{pmatrix},$$

这与定理 6 相抵触.

§9 $SL_n(K), GL_n(K), PSL_n(K)$ 和 $PGL_n(K)$ 的自同构 (特征数 = 2)

定理 1 设 $n\geqslant 2$, 而 K 的特征数 $=2$, 则 $SL_n(K)$ 的自同构必为形状

(1) $$A\to PA^\sigma P^{-1},$$

其中 σ 为 K 之自同构, P 为可逆; 或

(2) $$A\to P(A^{\tau\prime})^{-1}P^{-1},$$

其中 τ 为 K 之反自同构.

【证】 当 $n=2$ 时, 已知定理成立. 今对 n 施行归纳法.

先研究 $n=3$ 的情形. 设 $\mathscr{A}$ 为 $SL_3(K)$ 的自同构, 令

$$T_{ij}=I+E_{ij}\quad (i\neq j; 1\leqslant i,j\leqslant 3).$$

依定理 8.5, 不妨设

$$\mathscr{A}(T_{12})=T_{12},\quad \mathscr{A}(T_{21})=T_{21}.$$

由于

$$S_{12}=\begin{pmatrix} 0 & 1 & \\ 1 & 0 & \\ & & 1 \end{pmatrix}=T_{12}T_{21}T_{12},$$

所以也有

$$\mathscr{A}(S_{12}) = S_{12}.$$

考查 T_{13} 在 $\mathscr{A}$ 之下的像. 由 $T_{12}T_{13} = T_{13}T_{12}$ 及 $T_{13}^2 = I$ 推出

$$\mathscr{A}(T_{13}) = \begin{pmatrix} 1 & \lambda & \mu \\ & 1 & \\ & v & 1 \end{pmatrix},$$

其中 $\mu v = 0$. 由于

$$S_{12}T_{13} = \begin{pmatrix} 0 & 1 & 0 \\ 1 & 0 & 1 \\ 0 & 0 & 1 \end{pmatrix},$$

而

$$(S_{12}T_{13})^2 = \begin{pmatrix} 1 & 0 & 1 \\ 0 & 1 & 1 \\ 0 & 0 & 1 \end{pmatrix}$$

为对合, 故 $(\mathscr{A}(S_{12})\mathscr{A}(T_{13}))^2$ 为对合. 我们有

$$\mathscr{A}(S_{12})\mathscr{A}(T_{13}) = \begin{pmatrix} 0 & 1 & \\ 1 & 0 & \\ & & 1 \end{pmatrix}\begin{pmatrix} 1 & \lambda & \mu \\ & 1 & \\ & v & 1 \end{pmatrix} = \begin{pmatrix} 0 & 1 & 0 \\ 1 & \lambda & \mu \\ 0 & v & 1 \end{pmatrix}.$$

由

$$\begin{pmatrix} 0 & 1 & 0 \\ 1 & \lambda & \mu \\ 0 & v & 1 \end{pmatrix}^2 = \begin{pmatrix} 1 & \lambda & \mu \\ \lambda & 1+\lambda^2 & \lambda\mu+\mu \\ v & v\lambda+v & 1 \end{pmatrix}$$

为对合, 推出 $1+\lambda^2 = 1$, 故 $\lambda = 0$. 因此

$$\mathscr{A}(T_{13}) = \begin{pmatrix} 1 & 0 & \mu \\ & 1 & \\ & v & 1 \end{pmatrix},$$

其中 $\mu v = 0$. 分别研究 $\mu = 0$ 及 $v = 0$ 这两个情形.

(i)$v = 0$. 使 $\mathscr{A}$ 承受自同构

$$X \to \begin{pmatrix} 1 & & \\ & 1 & \\ & & \mu \end{pmatrix} X \begin{pmatrix} 1 & & \\ & 1 & \\ & & \mu \end{pmatrix}^{-1}$$

之后 (注意, 这个自同构不变 T_{12}, T_{21}), 还可以假定

$$\mathscr{A}(T_{13}) = T_{13}.$$

由于

$$T_{23} = S_{12}T_{13}S_{12}^{-1},$$

故也有

$$\mathscr{A}(T_{23}) = T_{23}.$$

考查 T_{31} 在 $\mathscr{A}$ 之下的像. 像前面一样, 由

$$T_{21}T_{31} = T_{31}T_{21}, \quad T_{31}^2 = I$$

及 $(S_{12}T_{31})^2$ 为对合推出

$$\mathscr{A}(T_{31}) = \begin{pmatrix} 1 & & \\ 0 & 1 & \gamma \\ \beta & & 1 \end{pmatrix},$$

其中 $\beta\gamma = 0$. 再由 T_{31} 与 T_{13} 不可换且 $(T_{31}T_{13})^3 = I$ 推出

$$\mathscr{A}(T_{31}) = T_{31},$$

于是也有

$$\mathscr{A}(T_{32}) = T_{32}.$$

考查

$$T_{12}(\lambda) = \begin{pmatrix} 1 & \lambda & \\ & 1 & \\ & & 1 \end{pmatrix} \quad (\lambda \in K^*)$$

在 $\mathscr{A}$ 之下的像. 由 $T_{12}(\lambda)$ 与 T_{12}, T_{13}, T_{32} 交换及 $T_{12}(\lambda)^2 = I$ 推出

$$\mathscr{A}(T_{12}(\lambda)) = \begin{pmatrix} 1 & \lambda^\sigma & \\ & 1 & \\ & & 1 \end{pmatrix}.$$

可是由

$$S_{23} = T_{23}T_{32}T_{23}$$

推出

$$\mathscr{A}(S_{23}) = S_{23},$$

于是由

$$T_{13}(\lambda) = S_{23}T_{12}(\lambda)S_{23}$$

及

$$T_{23}(\lambda) = S_{12}T_{13}(\lambda)S_{12}$$

推出

$$\mathscr{A}(T_{13}(\lambda)) = T_{13}(\lambda^\sigma),$$
$$\mathscr{A}(T_{23}(\lambda)) = T_{23}(\lambda^\sigma).$$

最后由

$$T_{12}(\lambda)T_{12}(\mu) = T_{12}(\lambda+\mu)$$

推出

$$(\lambda+\mu)^\sigma = \lambda^\sigma + \mu^\sigma.$$

再由

$$T_{12}(\lambda)T_{23}(\mu)T_{12}(\lambda)T_{23}(\mu) = T_{13}(\lambda\mu)$$

推出

$$(\lambda\mu)^\sigma = \lambda^\sigma\mu^\sigma.$$

因此 σ 为 K 之自同构.

因为 $SL_3(K)$ 由 $T_{12}(\lambda), T_{13}, T_{21}, T_{23}, T_{31}, T_{32}$ 生成, 故这时本定理成立.

(ii)$\mu = 0$. 使 $\mathscr{A}$ 承受自同构

$$X \to \begin{pmatrix} 1 & & \\ & 1 & \\ & & v \end{pmatrix}^{-1} X \begin{pmatrix} 1 & & \\ & 1 & \\ & & v \end{pmatrix}$$

之后 (注意这个自同构不变 T_{12}, T_{21}), 还可以假定

$$\mathscr{A}(T_{13}) = T_{32}.$$

再使 $\mathscr{A}$ 承受自同构

$$X \to \begin{pmatrix} 0 & 1 & \\ 1 & 0 & \\ & & 1 \end{pmatrix} X \begin{pmatrix} 0 & 1 & \\ 1 & 0 & \\ & & 1 \end{pmatrix}^{-1}$$

之后, 可设

$$\mathscr{A}(T_{12}) = T_{21}, \quad \mathscr{A}(T_{21}) = T_{12},$$
$$\mathscr{A}(T_{13}) = T_{31}, \quad \mathscr{A}(S_{12}) = S_{12}.$$

考查 T_{31} 在 $\mathscr{A}$ 之下的像. 像情形 (i) 一样, 由

$$T_{21}T_{31} = T_{31}T_{21}, \quad T_{31}^2 = I, (T_{31}T_{13})^3 = I$$

及 $(S_{12}T_{31})^2$ 为对合推出

$$\mathscr{A}(T_{31}) = T_{13},$$

于是也有

$$\mathscr{A}(T_{32}) = T_{23},$$

考查 $T_{12}(\lambda)$ 在 $\mathscr{A}$ 之下的像. 由 $T_{12}(\lambda)$ 与 T_{12}, T_{13}, T_{32} 交换推出

$$\mathscr{A}(T_{12}(\lambda)) = T_{21}(\lambda^\tau).$$

由

$$T_{12}(\lambda)T_{12}(\mu) = T_{12}(\lambda + \mu)$$

推出

$$(\lambda + \mu)^\tau = \lambda^\tau + \mu^\tau.$$

再由 $S_{23} = T_{23}T_{32}T_{23}$ 推出

$$\mathscr{A}(S_{23}) = S_{23}.$$

于是由 $T_{13}(\lambda) = S_{23}T_{12}(\lambda)S_{23}, T_{23}(\lambda) = S_{12}T_{13}(\lambda)S_{12}$ 推出

$$\mathscr{A}(T_{13}(\lambda)) = T_{31}(\lambda^\tau),$$
$$\mathscr{A}(T_{23}(\lambda)) = T_{32}(\lambda^\tau).$$

再由

$$T_{12}(\lambda)T_{23}(\mu)T_{12}(\lambda)T_{23}(\mu) = T_{13}(\lambda\mu)$$

推出

$$(\lambda\mu)^\tau = \mu^\tau\lambda^\tau,$$

因此 τ 为 K 之反自同构. 故这时本定理也成立.

以下研究 $n \geqslant 4$ 的情形. 设 $\mathscr{A}$ 为 $SL_n(K)$ 的自同构. 和 $n = 3$ 的情形一样, 不妨设

$$\mathscr{A}(T_{12}) = T_{12}, \quad \mathscr{A}(T_{21}) = T_{21}.$$

考查 $SL_n(K)$ 中与 T_{12} 及 T_{21} 交换的对合所生成的群 Γ, 它们由一切形如

$$\begin{pmatrix} \begin{matrix} 1 & 0 \\ 0 & 1 \end{matrix} & 0 \\ 0 & X_1 \end{pmatrix}$$

的元素组成, 其中 $X_1 \in SL_{n-2}(K)$. 易见 $\mathscr{A}(\Gamma)=\Gamma$. 因此 $\mathscr{A}$ 诱导出 $SL_{n-2}(K)$ 的一个自同构 $\mathscr{A}_1$:

$$\mathscr{A}\begin{pmatrix} \begin{matrix}1&0\\0&1\end{matrix} & 0 \\ 0 & X_1 \end{pmatrix} = \begin{pmatrix} \begin{matrix}1&0\\0&1\end{matrix} & 0 \\ 0 & \mathscr{A}_1(X_1) \end{pmatrix}.$$

依归纳法假设,

(*) $$\mathscr{A}_1(X_1)=P_1X_1^{\sigma}P_1^{-1},$$

其中 σ 为 K 之自同构, P_1 为 $(n-2)\times(n-2)$ 可逆矩阵; 或

(**) $$\mathscr{A}_1(X_1)=P_1(X_1^{\tau}{}')^{-1}P_1^{-1},$$

其中 τ 为 K 之反自同构. 如 (*) 发生, 使 $\mathscr{A}$ 承受自同构

$$X\to\left[\begin{pmatrix} I & \\ & P_1^{-1}\end{pmatrix} X \begin{pmatrix} I & \\ & P_1\end{pmatrix}\right]^{\sigma^{-1}};$$

如 (**) 发生, 使 $\mathscr{A}$ 承受自同构

$$X\to\left\{\left[\begin{pmatrix} I & \\ & P_1^{-1}\end{pmatrix} X \begin{pmatrix} I & \\ & P_1\end{pmatrix}\right]^{-1}\right\}^{\tau^{-1}\prime},$$

可设

$$\mathscr{A}\begin{pmatrix} I & 0\\ 0 & X_1\end{pmatrix}=\begin{pmatrix} I & 0\\ 0 & X_1\end{pmatrix},$$

对一切 $X_1\in SL_{n-2}(K)$.

先研究 $n=4$ 的情形. 考查 T_{23} 在 $\mathscr{A}$ 之下的像. 由

$$T_{21}T_{23}=T_{23}T_{21},\quad T_{23}T_{43}=T_{43}T_{23}$$

推出

$$\mathscr{A}(T_{23})=\begin{pmatrix} 1&0&0&0\\ \alpha&1&\beta&0\\ 0&0&1&0\\ \gamma&0&\delta&1\end{pmatrix}.$$

由于 $(S_{12}T_{23})^2$ 为对合, 故 $(\mathscr{A}(S_{12})\mathscr{A}(T_{23}))^2$ 亦然, 我们有

$$\mathscr{A}(S_{12})\mathscr{A}(T_{23})=\begin{pmatrix} 0&1&&\\ 1&0&&\\ &&1&\\ &&&1\end{pmatrix}\begin{pmatrix} 1&0&&\\ \alpha&1&\beta&0\\ &&1&\\ \gamma&0&\delta&1\end{pmatrix}=\begin{pmatrix} \alpha&1&\beta&0\\ 1&0&0&0\\ 0&0&1&0\\ \gamma&0&\delta&1\end{pmatrix}.$$

由

$$\begin{pmatrix} \alpha & 1 & \beta & 0 \\ 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ \gamma & 0 & \delta & 1 \end{pmatrix}^2 = \begin{pmatrix} \alpha^2+1 & \alpha & \alpha\beta+\beta & 0 \\ \alpha & 1 & \beta & 0 \\ 0 & 0 & 1 & 0 \\ \gamma\alpha+\gamma & \gamma & \gamma\beta & 1 \end{pmatrix}$$

为对合推出 $\alpha^2+1=1$, 故 $\alpha=0$. 同理, 由 $(S_{34}T_{23})^2$ 为对合推出 $\delta=0$. 因之

$$\mathscr{A}(T_{23}) = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & \beta & 0 \\ 0 & 0 & 1 & 0 \\ \gamma & 0 & 0 & 1 \end{pmatrix}.$$

再由 $(S_{12}S_{34}T_{23})^2$ 为对合, 推出 $(S_{12}S_{34}\mathscr{A}(T_{23}))^2$ 为对合. 注意

$$S_{12}S_{34}\mathscr{A}(T_{23}) = \begin{pmatrix} 0 & 1 & & \\ 1 & 0 & & \\ & & 0 & 1 \\ & & 1 & 0 \end{pmatrix}\begin{pmatrix} 1 & & & \\ & 1 & \beta & \\ & & 1 & \\ \gamma & & & 1 \end{pmatrix} = \begin{pmatrix} 0 & 1 & \beta & 0 \\ 1 & 0 & 0 & 0 \\ \gamma & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{pmatrix},$$

于是由

$$\begin{pmatrix} 0 & 1 & \beta & 0 \\ 1 & 0 & 0 & 0 \\ \gamma & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{pmatrix}^2 = \begin{pmatrix} 1+\beta\gamma & 0 & 0 & \beta \\ 0 & 1 & \beta & 0 \\ 0 & \gamma & \gamma\beta+1 & 0 \\ \gamma & 0 & 0 & 1 \end{pmatrix}$$

为对合推出 $\gamma\beta+1=1$. 所以 $\gamma\beta=0$. 分别研究 $\beta=0$ 及 $\gamma=0$ 这两种情形.

1° $\gamma=0$. 这时

$$\mathscr{A}(T_{23}) = \begin{pmatrix} 1 & & & \\ & 1 & \beta & \\ & & 1 & \\ & & & 1 \end{pmatrix}.$$

根据同样方法, 再根据 $(T_{23}T_{32})^3=I$ 推出

$$\mathscr{A}(T_{32}) = \begin{pmatrix} 1 & & & \\ & 1 & & \\ & \beta^{-1} & 1 & \\ & & & 1 \end{pmatrix}.$$

使 $\mathscr{A}$ 承受自同构

$$X \to \begin{pmatrix} \beta^{-1} & & & \\ & \beta^{-1} & & \\ & & 1 & \\ & & & 1 \end{pmatrix} X \begin{pmatrix} \beta^{-1} & & & \\ & \beta^{-1} & & \\ & & 1 & \\ & & & 1 \end{pmatrix}^{-1}$$

(注意, 此自同构不变 T_{12}, T_{21} 及 Γ 中元素) 之后, 可设

$$\mathscr{A}(T_{23}) = T_{23}, \quad \mathscr{A}(T_{32}) = T_{32}.$$

因 $SL_4(K)$ 由 $T_{12}, T_{21}, T_{23}, T_{32}, \Gamma$ 生成, 故这时定理成立.

2° $\beta = 0$. 这时

$$\mathscr{A}(T_{23}) = \begin{pmatrix} 1 & & & \\ & 1 & & \\ & & 1 & \\ \gamma & & & 1 \end{pmatrix}.$$

根据同样方法, 再根据 $(T_{23}T_{32})^3 = I$ 推出

$$\mathscr{A}(T_{32}) = \begin{pmatrix} 1 & & & \gamma^{-1} \\ & 1 & & \\ & & 1 & \\ & & & 1 \end{pmatrix}.$$

使 $\mathscr{A}$ 承受自同构

$$X \to \begin{pmatrix} \gamma & & & \\ & \gamma & & \\ & & 1 & \\ & & & 1 \end{pmatrix} X \begin{pmatrix} \gamma & & & \\ & \gamma & & \\ & & 1 & \\ & & & 1 \end{pmatrix}^{-1}$$

(注意此自同构不变 T_{12}, T_{21} 及 Γ 中元素) 之后, 可设

$$\mathscr{A}(T_{23}) = T_{41}, \quad \mathscr{A}(T_{32}) = T_{14}.$$

再使 $\mathscr{A}$ 承受自同构

$$X \to \begin{pmatrix} 0 & 1 & & \\ 1 & 0 & & \\ & & 0 & 1 \\ & & 1 & 0 \end{pmatrix} X \begin{pmatrix} 0 & 1 & & \\ 1 & 0 & & \\ & & 0 & 1 \\ & & 1 & 0 \end{pmatrix}$$

之后, 可设

$$\begin{aligned}
&\mathscr{A}(T_{12}) = T_{21}, && \mathscr{A}(T_{21}) = T_{12},\\
&\mathscr{A}(T_{23}) = T_{32}, && \mathscr{A}(T_{32}) = T_{23},\\
&\mathscr{A}(T_{34}(\lambda)) = T_{43}(\lambda), && \mathscr{A}(T_{43}(\lambda)) = T_{34}(\lambda).
\end{aligned}$$

由于

$$\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} = \begin{pmatrix} 1 & 1 \\ & 1 \end{pmatrix}\begin{pmatrix} 1 & \\ 1 & 1 \end{pmatrix}\begin{pmatrix} 1 & 1 \\ & 1 \end{pmatrix} = \begin{pmatrix} 1 & \\ 1 & 1 \end{pmatrix}\begin{pmatrix} 1 & 1 \\ & 1 \end{pmatrix}\begin{pmatrix} 1 & \\ 1 & 1 \end{pmatrix},$$

故

$$\begin{aligned}
&\mathscr{A}(S_{12}) = S_{12}, \quad \mathscr{A}(S_{23}) = S_{23},\\
&\mathscr{A}(S_{34}) = S_{34}.
\end{aligned}$$

由于

$$\begin{aligned}
S_{23}T_{34}(\lambda)S_{23} &= T_{24}(\lambda),\\
S_{34}T_{24}(\lambda)S_{34} &= T_{23}(\lambda),
\end{aligned}$$

故

$$\begin{aligned}
\mathscr{A}(T_{24}(\lambda)) &= T_{42}(\lambda),\\
\mathscr{A}(T_{23}(\lambda)) &= T_{32}(\lambda).
\end{aligned}$$

再由

$$T_{23}(\lambda)T_{34}(\mu)T_{23}(\lambda)T_{34}(\mu) = T_{24}(\lambda\mu)$$

推出

$$\begin{aligned}
&\mathscr{A}(T_{23}(\lambda))\mathscr{A}(T_{34}(\mu))\mathscr{A}(T_{23}(\lambda))\mathscr{A}(T_{34}(\mu))\\
&= T_{42}(\lambda\mu) = T_{32}(\lambda)T_{43}(\mu)T_{32}(\lambda)T_{43}(\mu) = T_{42}(\mu\lambda).
\end{aligned}$$

因此

$$\lambda\mu = \mu\lambda,$$

对一切 $\lambda, \mu \in K$, 即 K 是域. 那么使 $\mathscr{A}$ 承受自同构

$$X \to X'^{-1}$$

之后, 有

$$\begin{aligned}
&\mathscr{A}(T_{12}) = T_{12}, && \mathscr{A}(T_{21}) = T_{21},\\
&\mathscr{A}(T_{23}) = T_{23}, && \mathscr{A}(T_{32}) = T_{32},\\
&\mathscr{A}(T_{34}(\lambda)) = T_{34}(\lambda), && \mathscr{A}(T_{43}(\lambda)) = T_{43}(\lambda),
\end{aligned}$$

对一切 $\lambda \in K$. 因 $SL_4(K)$ 由 $T_{12}, T_{21}, T_{23}, T_{32}, T_{34}(\lambda), T_{43}(\lambda)(\lambda \in K)$ 所生成, 故这时定理也成立.

最后研究 $n \geqslant 5$ 的情形. 考查 T_{23} 在 $\mathscr{A}$ 之下的像. 因 T_{23} 与 $T_{ij}(4 \leqslant i, j \leqslant n), T_{21}, T_{43}$ 相交换, 故

$$\mathscr{A}(T_{23}) = \begin{pmatrix} 1 & 0 & 0 & \\ \lambda & 1 & \mu & 0 \\ 0 & 0 & 1 & \\ & 0 & & I \end{pmatrix}.$$

仿 $n=3$ 的情形, 可证 $\lambda = 0$. 因此

$$\mathscr{A}(T_{23}) = \begin{pmatrix} 1 & & & \\ & 1 & \mu & \\ & & 1 & \\ & & & I \end{pmatrix}.$$

同理可证

$$\mathscr{A}(T_{32}) = \begin{pmatrix} 1 & & & \\ & 1 & & \\ & v & 1 & \\ & & & I \end{pmatrix}.$$

因 $(T_{23}T_{32})^3 = I$, 故 $v = \mu^{-1}$. 使 $\mathscr{A}$ 承受自同构

$$X \to \begin{pmatrix} \mu^{-1} & & \\ & \mu^{-1} & \\ & & I \end{pmatrix} X \begin{pmatrix} \mu^{-1} & & \\ & \mu^{-1} & \\ & & I \end{pmatrix}^{-1}$$

(注意此自同构不变 T_{12}, T_{21} 及 Γ 中每个元素) 之后, 可设

$$\mathscr{A}(T_{23}) = T_{23}, \quad \mathscr{A}(T_{32}) = T_{32}.$$

因 $SL_n(K)$ 由 $\Gamma, T_{23}, T_{32}, T_{12}, T_{21}$ 生成, 故这时定理也成立.

至此定理完全证毕.

由上定理立刻推出

定理 2　设 $n \geqslant 2$, 而 K 的特征数为 2, 则 $GL_n(K)$ 的自同构必为形状

(3) $$A \to \chi(A) P A^{\sigma} P^{-1},$$

其中 σ 为 K 之自同构, P 为可逆矩阵, χ 为从 $GL_n(K)$ 到 K 之中心之中的同态映射且满足条件: 从 $\chi(\zeta I) = \zeta^{-1}$ 及 $\zeta \in Z^*$ 可得出 $\zeta = 1$; 或为形状

(4) $$A \to \chi(A) P (A^{\tau\prime})^{-1} P^{-1},$$

其中 τ 为 K 之反自同构.

为了确定 $PSL_n(K)$ 和 $PGL_n(K)$ 的自同构, 需要刻画出 1 对合来. 现在因 K 之特征数为 2, 这是很容易办到的.

设 A 和 B 为具有同样数量 γ 的两个互相交换的对合, 而 γ 不是 K 中中心元素的平方, 则

$$(AB)^2 = A^2B^2 = \gamma^2 I,$$

故 AB 决不与 A 和 B 共轭, 因此在 $PSL_n(K)$ 或 $PGL_n(K)$ 的自同构之下, 对合集 Γ_1 不变, 因之可得

定理 3 设 $n \geqslant 2, K$ 之特征数为 2, 则 $PSL_n(K)$(或 $PGL_n(K)$) 的自同构必为形状

(5) $$\bar{A} \to \bar{P}\,\bar{A}^{\sigma}\bar{P}^{-1},$$

其中 σ 为 K 之自同构, P 为可逆矩阵; 或

(6) $$\bar{A} \to \bar{P}(\overline{A^{\tau\prime}})^{-1}\bar{P}^{-1},$$

其中 τ 为 K 之反自同构.

第七章　H- 矩阵及酉群

§1　自反矩阵及 H- 矩阵

设 K 为体, 其特征数任意. 假定 K 有一个反自同构:

$$a \to \overline{a}.$$

我们先留意, 如果 A 为 K 上 $m \times n$ 矩阵, 而 B 是 K 上 $n \times 1$ 矩阵, 一般说来

$$(AB)' \neq B'A', \quad \overline{AB} \neq \overline{B}\,\overline{A};$$

但是, 我们永远有

(1) $$\overline{AB}' = \overline{B}'\overline{A}'.$$

其次, 设 A 是 K 上 $n \times n$ 矩阵; 如果 A 可逆, 一般说来, A' 和 $\bar{A}$ 都不一定可逆; 例如设 K 是实四元数体, $a \to \overline{a}$ 是通常的共轭, 取

$$A = \begin{pmatrix} 1 & i \\ j & k \end{pmatrix},$$

则

$$A' = \begin{pmatrix} 1 & j \\ i & k \end{pmatrix}, \quad \bar{A} = \begin{pmatrix} 1 & -i \\ -j & -k \end{pmatrix}$$

都不可逆. 但是如果 A 可逆, $\overline{A}'$ 也一定可逆, 而且

(2) $$(\overline{A}')^{-1} = (\overline{A^{-1}})'.$$

实际上, 依 (1), 我们有

$$\overline{A}'\,\overline{A^{-1}}' = \overline{A^{-1}A}' = I' = I.$$

设 A 和 B 是 K 上两个 $n \times n$ 矩阵. A 和 B 称为对于反自同构 $a \to \overline{a}$ 而言合同或简称合同, 如果有一个 K 上的可逆矩阵 P 存在, 使得

(3) $$A = PB\overline{P}'.$$

显然, 合同是一个等价关系, 而合同的矩阵有相同的秩.

设 A 是 K 上的一个 $n \times n$ 矩阵. 我们说两个 n 维行向量 x 和 y 对于 A 是正交的, 如果

$$xA\overline{y}' = 0.$$

A 称为自反矩阵, 如果对于任意 n 维行向量 x 和 y, 从 x 和 y 对于 A 正交都可以推出 y 和 x 对于 A 也正交, 即从 $xA\overline{y}'=0$ 推出 $yA\overline{x}'=0$. 我们来证明与自反矩阵合同的矩阵亦自反. 设 A 和 B 皆 K 上 $n\times n$ 矩阵, 而且合同, 即设 (3) 式成立. 假设 B 是自反矩阵. 设 x 和 y 是 n 维行向量而具有性质 $xA\overline{y}'=0$, 于是 $xPB\overline{P}'\overline{y}'=0$, 即 $(xP)B(\overline{y}P)'=0$. 因 B 自反, 故 $(yP)B(\overline{xP})'=0$, 于是 $yA\overline{x}'=yPB\overline{P}'\overline{x}'=0$. 因此 A 亦自反.

以下我们将局限于讨论自反矩阵. 首先我们证明

定理 1 设 A 为 K 上 $n\times n$ 自反矩阵, 其秩为 r, 那么一定存在着 K 上一个 $n\times n$ 可逆矩阵 P, 使得

$$PA\overline{P}'=\begin{pmatrix} A_1^{(r)} & 0 \\ 0 & 0^{(n-r)} \end{pmatrix},$$

其中 $A_1^{(r)}$ 为 K 上 $r\times r$ 可逆自反矩阵.

【证】 因 A 之秩为 r, 故有 K 上 $n\times n$ 可逆矩阵 P 存在, 使得

$$PA=\begin{pmatrix} B^{(r,n)} \\ 0^{(n-r,n)} \end{pmatrix}.$$

于是

$$PA\overline{P}'=\begin{pmatrix} A_1^{(r)} & A_2^{(r,n-r)} \\ 0 & 0^{(n-r)} \end{pmatrix}.$$

令

$$e_i=(0,\cdots,0,1,0\cdots,0)\quad(1\leqslant i\leqslant n).$$

那么 $e_{r+1},\cdots,e_n$ 与一切向量对于 $PA\overline{P}'$ 都正交. 因 A 自反, $PA\overline{P}'$ 亦自反, 故任一向量都与 $e_{r+1},\cdots,e_n$ 对于 $PA\overline{P}'$ 正交, 特别, $e_1,\cdots,e_r$ 与 $e_{r+1},\cdots,e_n$ 对于 $PA\overline{P}'$ 正交, 由此推出 $A_2=0$.

从定理 1 我们知道, 要研究自反矩阵在合同下不变的性质, 可以局限于研究可逆自反矩阵在合同下不变的性质.

现在设 A 是 K 上 $n\times n$ 可逆自反矩阵, 而 $n>1$. 则 $xA\overline{y}'=0$ 当且仅当 $yA\overline{x}'=0$ 对任意 n 维行向量 x 和 y. 因之 $xA\overline{y}'=0$ 当且仅当 $\overline{\overline{x}}\,\overline{A}'\overline{y}'=0$. 故当 x 固定时, 将 $\overline{y}_1,\cdots,\overline{y}_n$ 看作未定元, $xA\overline{y}'=0$ 和 $\overline{\overline{x}}\,\overline{A}'\overline{y}'=0$ 有相同的解. 因之有 $m_x\in K$ 存在, 使

$$xA=m_x\overline{\overline{x}}\,\overline{A}'.$$

设 x_1 和 x_2 在 K 上线性无关, 则

$$(x_1+x_2)A=m_{x_1+x_2}\overline{\overline{x_1+x_2}}\,\overline{A}'=m_{x_1+x_2}\overline{\overline{x}}_1\,\overline{A}'+m_{x_1+x_2}\overline{\overline{x}}_2\,\overline{A}'$$

$$= x_1A + x_2A = m_{x_1}\,\overline{\overline{x_1}}\,\overline{A}' + m_{x_2}\,\overline{\overline{x_2}}\,\overline{A}'.$$

又因为 x_1 和 x_2 在 K 上线性无关, $\overline{\overline{x_1}}$ 和 $\overline{\overline{x_1}}$ 在 K 上也线性无关, 于是从上式推出

$$m_{x_1+x_2} = m_{x_1} = m_{x_2}.$$

由此推出

(4) $$xA = m_0\,\overline{\overline{x}}\,\overline{A}',$$

其中 m_0 是 K 中与 x 无关的非零元素; 特别, $A = m_0\overline{A}'$. 由 (4) 式推知

(5) $$\overline{xA}' = \overline{\overline{A}}\,\overline{\overline{x}}'\overline{m}_0.$$

于是, 由 (4) 和 (5) 式有

$$\begin{aligned} xA\overline{y}' &= m_0\,\overline{\overline{x}}\,\overline{A}'\overline{y}' = m_0\,\overline{\overline{x}}\,\overline{yA}' \\ &= m_0\,\overline{\overline{x}}\,\overline{\overline{A}}\,\overline{\overline{y}}'\overline{m}_0 = m_0(\overline{\overline{xA\overline{y}'}})\overline{m}_0. \end{aligned}$$

因对任意 n 维行向量 x 和 y 上式都成立, 而 K 中任一元素皆可表成形状 $xA\overline{y}'$, 故

$$a = m_0\,\overline{\overline{a}}\,\overline{m}_0, 对一切 a \in K.$$

特别, 当 $a = 1$ 时有

$$m_0\overline{m}_0 = 1.$$

分别研究以下两种情形:

(i)$a = -m_0\overline{a}$, 对一切 $a \in K$. 令 $a = 1$, 就有 $m_0 = -1$; 因此 $\overline{a} = a$, 这就是说 K 是域, $a \to \overline{a}$ 是 K 的单位自同构, 而 A 具有性质

$$A' = -A,$$

这时 A 称为斜对称矩阵.

(ii)K 中有一个元素 $a \neq 0$ 具有性质 $a \neq -m_0\overline{a}$. 令 $q = a + m_0\overline{a}$, 则 $q \neq 0$, 而 $m_0\overline{q} = m_0(\overline{a} + \overline{\overline{a}}\,\overline{m}_0) = m_0\overline{a} + m_0\,\overline{\overline{a}}\,\overline{m}_0 = a + m_0\overline{a} = q$. 如果令 $\widetilde{a} = (\overline{qaq^{-1}})$ 及 $B = q^{-1}A$, 则 $a \to \widetilde{a}$ 也是 K 的反自同构, 而且

(6) $$\widetilde{\widetilde{a}} = a, 对一切 a \in K$$

及

(7) $$\widetilde{B}' = B.$$

实际上,

$$\begin{aligned} \widetilde{\widetilde{a}} &= (\overline{q(\overline{qaq^{-1}})q^{-1}}) = \overline{q}^{-1}(\overline{\overline{qaq^{-1}}})\overline{q} = \overline{q}^{-1}\overline{\overline{q}}\,\overline{\overline{a}}\,\overline{\overline{q}}^{-1}\overline{q} \\ &= \overline{q}^{-1}\overline{q}\;\overline{m}_0^{-1}\,\overline{\overline{a}}\,\overline{m}_0\overline{q}^{-1}\overline{q} = m_0\,\overline{\overline{a}}\,\overline{m}_0 = a, \end{aligned}$$

而

$$\widetilde{B}' = \overline{qBq^{-1}}' = \overline{Aq^{-1}}' = \overline{q}^{-1}\overline{A}' = q^{-1}m_0\overline{A}' = q^{-1}A = B.$$

我们把适合条件 (6) 的反自同构称为 K 的对合性反自同构, 或简称为对合. 我们还把适合条件 (7) 的矩阵 B 称为对于对合 $a \to \widetilde{a}$ 而言的 Hamilton 矩阵, 或简称为哈矩阵.

最后, 我们注意, 如果 A_1 和 A_2 为 K 上对于反自同构 $a \to \overline{a}$ 的自反矩阵, 而且 A_1 和 A_2 对于反自同构 $a \to \overline{a}$ 而言是合同的, 则 $B_1 = q^{-1}A_1$ 和 $B_2 = q^{-1}A_2$ 是 K 上对于对合 $a \to \widetilde{a}$ 的哈矩阵, 而且 B_1 和 B_2 对于对合 $a \to \widetilde{a}$ 而言是合同的. 实际上, 如 $A_1 = PA_2\overline{P}'$, 则

$$B_1 = (q^{-1}Pq)B_2\widetilde{(q^{-1}Pq)}'.$$

因此, 具反自同构的体 K 上可逆自反矩阵的研究化归为域上可逆斜对称矩阵的研究和体上可逆哈矩阵的研究.

我们举出一些 Hamilton 矩阵的例子.

【例 1】 设 K 是域, 而 $a \to \overline{a}$ 是 K 的单位自同构, 即 $\overline{a} = a$ 对一切 $a \in K$. 这时, K 上的对于单位自同构的哈矩阵 H 适合条件

$$H' = H,$$

我们把它称为对称矩阵. 注意, 当 K 的特征数为 2 时, 对称矩阵与斜对称矩阵并无区别.

【例 2】 设 K 为域而 $a \to \overline{a}$ 是 K 的一个 2 阶的自同构. 这时 K 上哈矩阵 H 称为 Hermite 矩阵.

【例 3】 设 K 为广义四元数体, 而 $a \to \overline{a}$ 为 K 的共轭. 这时 K 上哈矩阵即是通常的哈矩阵.

今设 K 为体, 而 $a \to \overline{a}$ 为 K 的一个对合. 相应于 K 上哈矩阵, 我们定义 K 上一个 $n \times n$ 矩阵 H 为对于这个对合的斜 Hamilton 矩阵, 或简称斜哈矩阵, 如果

$$\overline{H}' = -H.$$

显然, 域上的斜对称矩阵是斜哈矩阵的特殊例子. 而当 K 的特征数为 2 时, K 上的斜哈矩阵与哈矩阵并无区别. 我们举出一些斜哈矩阵的例子.

【例 4】 设 K 是域, 而 $a \to \overline{a}$ 是 K 的一个 2 阶自同构. 这时 K 上斜哈矩阵称为斜 Hermite 矩阵.

【例 5】 设 K 为广义四元数体, 而 $a \to \overline{a}$ 为 K 的共轭. 这时 K 上斜哈矩阵即是通常的斜哈矩阵.

仍设 K 为体, 而 $a \to \overline{a}$ 为 K 的一个对合. K 中元素 α 具有性质 $\overline{\alpha} = \alpha$ 者称为 K 中对称元素, 而 K 中元素 α 具有性质 $\overline{\alpha} = -\alpha$ 者称为 K 中斜对称元素. 当 K 的特征数为 2 时, 对称元素与斜对称元素并无区别. 显然, K 一定有非 0 对称元素, 例如 K 的单位元素 1 即是. 另一方面, 如 $a \to \overline{a}$ 不是单位自同构, K 恒有斜对称元素. 实际上, 设 $a \in K$, 而 $\overline{a} \neq a$, 于是 $a - \overline{a}$ 就是 K 的一个非零斜对称元素. 设 H 是 K 上哈矩阵 (或斜哈矩阵) 而 α 是 K 中非零对称元素 (或斜对称元素), 则 $a \to \widetilde{a} = \alpha^{-1}\overline{a}\alpha$ 仍是 K 的一个对合. 如令 $H_1 = \alpha^{-1}H$, 则

$\widetilde{H}_1' = H_1$, 如果 H 是哈矩阵, 而 α 是对称元素,

　　或 H 是斜哈矩阵, 而 α 是斜对称元素;

$\widetilde{H}_1' = -H_1$, 如果 H 是哈矩阵, 而 α 是斜对称元素,

　　或 H 是斜哈矩阵, 而 α 是对称元素.

因此, 当 $a \to \overline{a}$ 不是 K 的单位自同构时, 哈矩阵的研究与斜哈矩阵的研究是一回事.

现在我们引进迹式哈矩阵的概念. 设 K 是具对合 $a \to \overline{a}$ 的体, K 上一个 $n \times n$ 对于对合 $a \to \overline{a}$ 的哈矩阵 H 称为迹式哈矩阵, 如果对任何 n 维向量 $x, xH\overline{x}'$ 皆可表成形式 $a + \overline{a}$, 而 $a \in K$. 当 K 的特征数 $\neq 2$ 时, 哈矩阵皆迹式哈矩阵. 实际上, 如 H 为哈矩阵, 而 x 为任意 n 维向量, 令 $a = \dfrac{1}{2}xH\overline{x}'$, 则 $\overline{a} = a$, 因而 $xH\overline{x}' = a + \overline{a}$. 如 K 的特征数 $= 2$, 而 K 的中心 Z 中的对称元素组成的子域 $Z_0 \neq Z$ 时 (这时对合称为第二类对合, 而相反情形, 对合则称为第一类对合), 哈矩阵也是迹式哈矩阵. 实际上, 这时存在着一个元素 $\gamma \in Z$, 而 $\overline{\gamma} \neq \gamma$, 于是 $\alpha = \gamma + \overline{\gamma} \neq 0$; 如果 μ 是 K 中任一对称元素, 因 $\alpha \in Z$, 我们有 $\overline{\alpha^{-1}\mu} = \alpha^{-1}\mu$, 因此 $\mu = \gamma(\alpha^{-1}\mu) + \overline{\gamma}(\overline{\alpha^{-1}\mu})$; 由此即可推出哈矩阵皆迹式. 最后, 如果 K 是特征数为 2 的域, 而 $a \to \overline{a}$ 是单位自同构, 这时的确存在着非迹式的哈矩阵 (对称矩阵), 例如

$$\begin{pmatrix} 1 & 0 & 0 \\ 0 & 0 & 1 \\ 0 & 1 & 0 \end{pmatrix}$$

即是. 这时对称矩阵 H 是迹式的, 当且仅当

(8)　　$xH\overline{x}' = 0,$ 对一切n维行向量.

我们把域 K 上适合条件 (8) 的斜对称矩阵 H 称为交错矩阵. 于是, 特征数 $\neq 2$ 的域 K 上的斜对称矩阵都是交错矩阵, 而特征数 $= 2$ 的域 K 上的斜对称矩阵是交错矩阵, 当且仅当它是迹式的.

最后, 为了简便起见, 我们把特征数 $\neq 2$ 的具对合 $a \to \overline{a}$ 的体 K 上的斜哈矩阵及特征数任意的具对合 $a \to \overline{a}$ 的体 K 上的迹式哈矩阵统称为对于对合 $a \to \overline{a}$

的 H- 矩阵. 设 H 为对于对合 $a \to \overline{a}$ 的 H- 矩阵, 则

$$\overline{H}' = \rho H,$$

而 $\rho = \pm 1, \rho$ 称为 H 的标元. 在以下讨论中, 除非另有声明, 我们约定 K 的对合 $a \to \overline{a}$ 是取定的. 于是对于对合 $a \to \overline{a}$ 的 H- 矩阵就简称为 H- 矩阵.

§2 H- 矩阵在合同下的化简

命

$$H = \begin{pmatrix} H_1 & L \\ \rho\overline{L}' & H_2 \end{pmatrix} \quad (\rho = \pm 1)$$

是一 $n \times n$ H- 矩阵, 而 $H_1 = H_1^{(r)}$ 可逆, 则

$$(1) \qquad \begin{pmatrix} I^{(r)} & 0 \\ -\rho\overline{L}'H_1^{-1} & I^{(n-r)} \end{pmatrix} \begin{pmatrix} H_1 & L \\ \rho\overline{L}' & H_2 \end{pmatrix} \overline{\begin{pmatrix} I^{(r)} & 0 \\ -\rho\overline{L}'H_1^{-1} & I^{(n-r)} \end{pmatrix}}' = \begin{pmatrix} H_1 & 0 \\ 0 & H_2 - \rho\overline{L}'H_1^{-1}L \end{pmatrix}.$$

这个公式对于 H- 矩阵在合同下的化简非常有用.

我们先从交错矩阵开始讨论. 我们注意交错矩阵的对角线上元素皆零.

定理 1 设 K 为域, 而 H 为 K 上 $n \times n$ 交错矩阵. 设 H 的秩为 r, 则 r 必为偶数, 而 H 必合同于

$$(2) \qquad \begin{pmatrix} \begin{matrix} 0 & 1 \\ -1 & 0 \end{matrix} & & & & & & \\ & \begin{matrix} 0 & 1 \\ -1 & 0 \end{matrix} & & & & 0 & \\ & & \ddots & & & & \\ & & & \begin{matrix} 0 & 1 \\ -1 & 0 \end{matrix} & & & \\ & & & & 0 & & \\ & 0 & & & & \ddots & \\ & & & & & & 0 \end{pmatrix} \quad (\tfrac{r}{2}\text{个}\ \begin{matrix} 0 & 1 \\ -1 & 0 \end{matrix}).$$

【证】 用归纳法向 n 证之. 当 $n = 1$ 时, $H = (0)$, 本定理自然成立. 次设 $n = 2$, 这时

$$H = \begin{pmatrix} 0 & h_{12} \\ -h_{12} & 0 \end{pmatrix}.$$

如 $h_{12} = 0$, 本定理自然成立; 否则 H 合同于

$$\begin{pmatrix} 1 & 0 \\ 0 & h_{12}^{-1} \end{pmatrix} H \begin{pmatrix} 1 & 0 \\ 0 & h_{12}^{-1} \end{pmatrix}' = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix},$$

因此本定理也成立. 今设 $n>2$, 而定理对于 $m<n$ 皆成立.

设

$$H=\begin{pmatrix} 0 & h_{12} & h_{13} & \cdots & h_{1n} \\ -h_{12} & 0 & h_{23} & \cdots & h_{2n} \\ -h_{13} & -h_{23} & 0 & \cdots & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ -h_{1n} & -h_{2n} & 0 & \cdots & 0 \end{pmatrix}.$$

如 $H=0$, 本定理自然成立. 设 $H\neq 0$, 于是不妨设 $h_{12}\neq 0$; 否则 H 必合同于一个矩阵, 它的 (1, 2) 位置元素不为 0. 实际上, 如 $h_{ij}\neq 0$, 而 $i<j$, 将 H 的第一列与第 i 列对调, 然后再将第一行与第 i 行对调即得一与 H 合同的矩阵 H_1, 它的 $(1,j)$ 位置元素不为 0; 将 H_1 的第二列与第 j 列对调, 然后再将第二行与第 j 行对调, 即得一与 H 合同的矩阵, 它的 (1, 2) 位置元素不为 0. 令

$$H_1=\begin{pmatrix} 0 & h_{12} \\ -h_{12} & 0 \end{pmatrix},$$

则 H_1 可逆. 依 (1) 式, H 合同于以下形状的交错矩阵:

$$\begin{pmatrix} 0 & h_{12} & 0 \\ -h_{12} & 0 & 0 \\ 0 & 0 & H_2 \end{pmatrix},$$

H_2 亦为交错矩阵. 于是 H 合同于

$$\begin{pmatrix} \begin{matrix} 1 & 0 \\ 0 & h_{12}^{-1} \end{matrix} & 0 \\ 0 & I^{(n-2)} \end{pmatrix} \begin{pmatrix} \begin{matrix} 0 & h_{12} \\ -h_{12} & 0 \end{matrix} & 0 \\ 0 & H_2 \end{pmatrix} \begin{pmatrix} \begin{matrix} 1 & 0 \\ 0 & h_{12}^{-1} \end{matrix} & 0 \\ 0 & I^{(n-2)} \end{pmatrix}'$$
$$=\begin{pmatrix} \begin{matrix} 0 & 1 \\ -1 & 0 \end{matrix} & 0 \\ 0 & H_2 \end{pmatrix}.$$

依归纳法假设, H_2 合同于

$$PH_2P'=\begin{pmatrix} \begin{matrix} 0 & 1 \\ -1 & 0 \end{matrix} & & & & & 0 \\ & \ddots & & & & \\ & & \begin{matrix} 0 & 1 \\ -1 & 0 \end{matrix} & & & \\ & & & 0 & & \\ & & & & \ddots & \\ 0 & & & & & 0 \end{pmatrix}\ (s\text{个}),\quad P=P^{(n-2)}\text{可逆}.$$

因此,H 合同于

$$\begin{pmatrix} I^{(2)} & 0 \\ 0 & P \end{pmatrix}\begin{pmatrix} 0 & 1 & 0 \\ -1 & 0 & \\ & 0 & H_2 \end{pmatrix}\begin{pmatrix} I^{(2)} & 0 \\ 0 & P \end{pmatrix}' = \begin{pmatrix} \begin{matrix} 0 & 1 \\ -1 & 0 \end{matrix} & & & & & \\ & \ddots & & & & 0 \\ & & \begin{matrix} 0 & 1 \\ -1 & 0 \end{matrix} & & & \\ & & & 0 & & \\ & 0 & & & \ddots & \\ & & & & & 0 \end{pmatrix} \quad (s+1\text{个}).$$

于是 H 的秩 $r = 2(s+1)$ 为偶数. 本定理完全证毕.

系理 1 设 K 为域, K 上两个 $n \times n$ 交错矩阵合同, 当且仅当它们同秩.

这样, 交错矩阵的合同问题就完满地解决了. (2) 即是秩为 r 的交错矩阵的标准形.

系理 2 设 K 为域, K 上交错矩阵的行列式一定是 K 中的平方数.

【证】 设 H 为 K 上 $n \times n$ 交错矩阵. 如 H 的秩 $r < n$, 则显然 $\det H = 0$. 如 H 的秩为 n, 则依定理 1, n 为偶数, 而且有 $n \times n$ 可逆矩阵 P 存在, 使

$$PHP' = \begin{pmatrix} \begin{matrix} 0 & 1 \\ -1 & 0 \end{matrix} & & 0 \\ & \ddots & \\ 0 & & \begin{matrix} 0 & 1 \\ -1 & 0 \end{matrix} \end{pmatrix}.$$

于是 $\det H = (\det P)^{-2}$. 无论在哪种情形, $\det H$ 都是平方数.

当 $\det \mathrm{H} \neq 0$, 具体计算出 $\det H$ 是表达式, 是一个有意思的问题.

定理 2 设

$$A = \begin{pmatrix} 0 & a_{12} & a_{13} & \cdots & a_{1n} \\ -a_{12} & 0 & a_{23} & \cdots & a_{2n} \\ -a_{13} & -a_{23} & 0 & \cdots & a_{3n} \\ \vdots & \vdots & \vdots & & \vdots \\ -a_{1n} & -a_{2n} & -a_{3n} & \cdots & 0 \end{pmatrix}$$

是域 K 上 $n = 2\nu$ 行的可逆交错矩阵, 则可将 $\det A$ 表作

$$\det A = [\gamma(A)]^2,$$

其中

$$\gamma(A)=\frac{1}{\nu!}\sum_{\substack{\begin{pmatrix}1&2&\cdots&n\\ i_1&i_2&\cdots&i_n\end{pmatrix}\in\mathfrak{S}_n\\ i_1<i_2,\cdots,i_{n-1}<i_n}}\operatorname{sgn}\begin{pmatrix}1&2&\cdots&n\\ i_1&i_2&\cdots&i_n\end{pmatrix}a_{i_1i_2}a_{i_3i_4}\cdots a_{i_{n-1}i_n}.$$

【证】 我们对 ν 用归纳法. 当 $\nu=1$ 时定理显然成立. 现在设 $\nu>1$. 先假定 $a_{12}\neq 0$. 那么写

$$A=\begin{pmatrix}A_{11}&A_{12}\\ -A_{12}'&A_{22}\end{pmatrix},$$

其中 $A_{11}=\begin{pmatrix}0&a_{12}\\ -a_{12}&0\end{pmatrix}$ 可逆, A_{12} 为 $2\times(n-2)$ 矩阵, A_{22} 为 $(n-2)\times(n-2)$ 矩阵. 于是由

$$\begin{pmatrix}I^{(2)}&0\\ A_{12}'A_{11}^{-1}&I\end{pmatrix}\begin{pmatrix}A_{11}&A_{12}\\ -A_{12}'&A_{22}\end{pmatrix}\begin{pmatrix}I^{(2)}&0\\ A_{12}'A_{11}^{-1}&I\end{pmatrix}'=\begin{pmatrix}A_{11}&0\\ 0&A_{12}'A_{11}^{-1}A_{12}+A_{22}\end{pmatrix}$$

及归纳法假设, 推知

$$\det A=a_{12}^2[\gamma(A_{12}'A_{11}^{-1}A_{12}+A_{22})]^2.$$

我们要证明

$$\gamma(A)=a_{12}\gamma(A_{12}'A_{11}^{-1}A_{12}+A_{22}).$$

令

$$A_{12}'A_{11}^{-1}A_{12}+A_{22}=(b_{ij})_{3\leqslant i,j\leqslant n},$$

则

$$b_{ij}=a_{2i}a_{12}^{-1}a_{1j}-a_{1i}a_{12}^{-1}a_{2j}+a_{ij}.$$

于是

$$\begin{aligned}&a_{12}\gamma(A_{12}'A_{11}^{-1}A_{12}+A_{22})\\ =&\frac{a_{12}}{(\nu-1)!}\sum_{\substack{\begin{pmatrix}3&4&\cdots&n\\ i_3&i_4&\cdots&i_n\end{pmatrix}\in\mathfrak{S}_{n-2}\\ i_3<i_4,\cdots,i_{n-1}<i_n}}\operatorname{sgn}\begin{pmatrix}3&4&\cdots&n\\ i_3&i_4&\cdots&i_n\end{pmatrix}b_{i_3i_4}\cdots b_{i_{n-1}i_n}.\end{aligned}$$

不难利用直接展开来验证

$$\sum_{\substack{\begin{pmatrix} j_{s-1} & j_s & j_{t-1} & j_t \\ i_{s-1} & i_s & i_{t-1} & i_t \end{pmatrix} \in \mathfrak{S}_4 \\ i_{s-1}<i_s, i_{t-1}<i_t}} \operatorname{sgn}\begin{pmatrix} j_{s-1} & j_s & j_{t-1} & j_t \\ i_{s-1} & i_s & i_{t-1} & i_t \end{pmatrix} (a_{2i_{s-1}}\alpha_{1i_s} - a_{1i_{s-1}}a_{2i_s})$$

$$\cdot (a_{2i_{t-1}}\alpha_{1i_t} - a_{1i_{t-1}} - a_{2i_t}) = 0.$$

对于 3 与 n 之间的 4 个不同的足码 $j_{s-1}, j_s, j_{t-1}, j_t$ 连续运用这个恒等式, 我们得到

$$\begin{aligned}
&a_{12}\gamma(A'_{12}A_{11}^{-1}A_{12} + A_{22}) \\
&= \frac{a_{12}}{(\nu-1)!} \sum_{\substack{\begin{pmatrix} 3 & 4 & \cdots & n \\ i_3 & i_4 & \cdots & i_n \end{pmatrix} \in \mathfrak{S}_{n-2} \\ i_3<i_4,\cdots,i_{n-1}<i_n}} \operatorname{sgn}\begin{pmatrix} 3 & 4 & \cdots & n \\ i_3 & i_4 & \cdots & i_n \end{pmatrix} \\
&\cdot \left\{ \sum_{s=4,6,\cdots,n} [a_{i_3i_4} \cdots (a_{2i_{s-1}}a_{12}^{-1}a_{1_i}, -a_{2i_s}a_{12}^{-1}a_{1i_{s-1}}) \cdots a_{i_{n-1}i_n}] + a_{i_3i_4} \cdots a_{i_{n-1}i_n} \right\} \\
&= \frac{a_{12}}{(\nu-1)!} \sum_{\substack{\begin{pmatrix} 3 & 4 & \cdots & n \\ i_3 & i_4 & \cdots & i_n \end{pmatrix} \in \mathfrak{S}_{n-2} \\ i_3<i_4,\cdots,i_{n-1}<i_n}} \operatorname{sgn}\begin{pmatrix} 3 & 4 & \cdots & n \\ i_3 & i_4 & \cdots & i_n \end{pmatrix} \\
&\cdot \sum_{s=4,6,\cdots,n} a_{i_3i_4} \cdots a_{2i_{s-1}}a_{12}^{-1}a_{1i_s} \cdots a_{i_{n-1}i_n} \\
&+ \left\{ \sum_{\substack{\begin{pmatrix} 3 & 4 & \cdots & n \\ i_3 & i_4 & \cdots & i_n \end{pmatrix} \in \mathfrak{S}_{n-2} \\ i_3<i_4,\cdots,i_{n-1}<i_n}} \operatorname{sgn}\begin{pmatrix} 3 & 4 & \cdots & n \\ i_3 & i_4 & \cdots & i_n \end{pmatrix} a_{i_3i_4} \cdots a_{i_{n-1}i_n} \right\} \\
&= \frac{1}{\nu!} \sum_{\substack{\begin{pmatrix} 1 & 2 & \cdots & n \\ i_1 & i_2 & \cdots & i_n \end{pmatrix} \in \mathfrak{S}_n \\ i_1<i_2,\cdots,i_{n-1}<i_n}} \operatorname{sgn}\begin{pmatrix} 1 & 2 & \cdots & n \\ i_1 & i_2 & \cdots & i_n \end{pmatrix} a_{i_1i_2} \cdots a_{i_{n-1}i_n} = \gamma(A).
\end{aligned}$$

现在研究 $a_{12} = 0$ 的情形. 这时有一个足码 $k > 2$ 存在, 使 $a_{1k} \neq 0$. 令

$$P=\begin{pmatrix} 1 & & & & & & & \\ & 0 & & \cdots & 1 & \cdots & & \\ & & 1 & & & & & \\ & \vdots & & \ddots & \vdots & & & \\ & & & & 1 & & & \\ & -1 & & \cdots & 0 & \cdots & & \\ & & & & & 1 & & \\ & & & & & & \ddots & \\ & & & & & & & 1 \end{pmatrix}\begin{matrix} \\ \text{第 2 行} \\ \\ \\ \\ \text{第 } k \text{ 行} \\ \\ \\ \\ \end{matrix},$$

则 PAP' 为一交错矩阵, 其 (1, 2) 位置元素 $\neq 0$. 写

$$PAP' = (b_{ij}),$$

则

$$\begin{aligned} &b_{ij} = a_{ij} \quad (i \neq 2, k;\ j \neq 2, k), \\ &b_{i2} = a_{ik}, \quad b_{ik} = -a_{i2} \quad (i \neq 2, k), \\ &b_{2k} = a_{2k}. \end{aligned}$$

于是

$$\begin{aligned} \gamma(PAP') &= \frac{1}{\nu!} \sum_{\substack{\begin{pmatrix} 1 & 2 & \cdots & n \\ i_1 & i_2 & \cdots & i_n \end{pmatrix} \in \mathfrak{S}_n \\ i_1<i_2,\cdots,i_{n-1}<i_n}} \operatorname{sgn}\begin{pmatrix} 1 & 2 & \cdots & n \\ i_1 & i_2 & \cdots & i_n \end{pmatrix} b_{i_1i_2}\cdots b_{i_{n-1}i_n} \\ &= \frac{1}{\nu!} \sum_{\begin{pmatrix} 1 & 2 & \cdots & n \\ i_1 & i_2 & \cdots & i_n \end{pmatrix} \in \mathfrak{S}_n} \operatorname{sgn}\begin{pmatrix} 1 & 2 & \cdots & n \\ i_1 & i_2 & \cdots & i_n \end{pmatrix} a_{i_1i_2}\cdots a_{i_{n-1}i_n} = \gamma(A). \end{aligned}$$

因之

$$\det A = \det(PAP') = [\gamma(PAP')]^2 = [\gamma(A)]^2.$$

由定理 2 可以推出

定理 3　设 A_1 和 A_2 是域 K 上两个 $n = 2\nu$ 次的可逆交错矩阵. 设 P 为 $n \times n$ 可逆矩阵使

$$PA_1P' = A_2,$$

则

$$\gamma(A_2) = (\det P)\gamma(A_1).$$

【证】 令

$$A_1 = (a_{ij}), A_2 = (b_{ij}), P = (p_{ij}),$$

则

$$b_{ij} = \sum_{s,t=1}^{n} p_{is} a_{st} p_{jt}.$$

于是

$$\gamma(A_2) = \frac{1}{\nu!} \sum_{\substack{\begin{pmatrix} 1 & 2 & \cdots & n \\ i_1 & i_2 & \cdots & i_n \end{pmatrix} \in \mathfrak{S}_n \\ i_1 < i_2, \cdots, i_{n-1} < i_n}} \operatorname{sgn} \begin{pmatrix} 1 & 2 & \cdots & n \\ i_1 & i_2 & \cdots & i_n \end{pmatrix} b_{i_1 i_2} \cdots b_{i_{n-1} i_n}$$

$$= \frac{1}{\nu!} \sum_{\substack{\begin{pmatrix} 1 & 2 & \cdots & n \\ i_1 & i_2 & \cdots & i_n \end{pmatrix} \in \mathfrak{S}_n \\ i_1 < i_2, \cdots, i_{n-1} < i_n}} \operatorname{sgn} \begin{pmatrix} 1 & 2 & \cdots & n \\ i_1 & i_2 & \cdots & i_n \end{pmatrix}$$

$$\cdot \left(\sum_{s_1, s_2} p_{i_1 s_1} a_{s_1 s_2} p_{i_2 s_2} \right) \cdots \left(\sum_{s_{n-1}, s_n} p_{i_{n-1} s_{n-1}} a_{s_{n-1} s_n} p_{i_n s_n} \right)$$

$$= \frac{1}{\nu!} \sum_{\begin{pmatrix} 1 & 2 & \cdots & n \\ s_1 & s_2 & \cdots & s_n \end{pmatrix} \in \mathfrak{S}_n} \operatorname{sgn} \begin{pmatrix} 1 & 2 & \cdots & n \\ s_1 & s_2 & \cdots & s_n \end{pmatrix}$$

$$\cdot \left[\sum_{\begin{pmatrix} s_1 & \cdots & s_n \\ i_1 & \cdots & i_n \end{pmatrix} \in \mathfrak{S}_n} \operatorname{sgn} \begin{pmatrix} s_1 & \cdots & s_n \\ i_1 & \cdots & i_n \end{pmatrix} p_{i_1 s_1} \cdots p_{i_n s_n} \right] a_{s_1 s_2} \cdots a_{s_{n-1} s_n}$$

$$= (\det P) \gamma(A_1).$$

系理 设 A 为域 K 上 $n = 2\nu$ 次的可逆交错矩阵. 设 P 为 K 上矩阵, 适合条件

$$PAP' = A,$$

则

$$\det P = 1.$$

§3　H- 矩阵在合同下的化简 (续)

如果 H- 矩阵不是交错矩阵, 合同问题并不像交错矩阵那样解决得好, 然而我们总有

定理 1　设 K 为具对合 $a \to \overline{a}$ 的体, 而 H 为 K 上 $n \times n$ H- 矩阵, 并假设 H 不是交错矩阵. 则 H 一定和一个对角形 H- 矩阵合同.

【证】　当 $n=1$ 时, 定理显然成立. 今用归纳法来证明本定理. 分两种情形进行:

(i) 若 H 中有一对角线元素不等于 0, 不失普遍性, 不妨假定 (1, 1) 位置上元素不等于 0. 于 §2(1) 中, 取 $r=1$. 由归纳法假设, 可得定理.

(ii)H 的对角线上元素都等于 0. 则 H 或者是零矩阵, 或者有一非对角线的元素不等于零. 对于前者显然定理成立; 对于后者, 可以假定其非 0 元素 a 在 (1, 2) 位置处. 于 (2.1) 中取 $r=2$, 则 H 与

$$H_1 = \begin{pmatrix} 0 & a \\ \rho\overline{a} & 0 \end{pmatrix} \text{ 及 } H_2 - \rho\overline{L}'H_1^{-1}L$$

的直和所成的方阵合同. 因为

$$\begin{pmatrix} 1 & \lambda \\ & 1 \end{pmatrix}\begin{pmatrix} 0 & a \\ \rho\overline{a} & 0 \end{pmatrix}\overline{\begin{pmatrix} 1 & \lambda \\ & 1 \end{pmatrix}}' = \begin{pmatrix} \lambda\rho\overline{a}+a\overline{\lambda} & * \\ * & * \end{pmatrix}.$$

如可求得 $\lambda \neq 0$, 使 $\lambda\rho\overline{a}+a\overline{\lambda} \neq 0$, 即化归情形 (i). 于是定理成立. 假定对所有 λ, 常有

$$\lambda\rho\overline{a}+a\overline{\lambda}=0.$$

命 $\lambda=1$, 即得 $\rho\overline{a}+a=0$. 于是对所有 λ,

$$\overline{\lambda}=a^{-1}\lambda a.$$

因为 $\lambda \to \overline{\lambda}$ 为 K 的反自同构, 而 $\overline{\lambda}=a^{-1}\lambda a$ 是 K 的自同构, 所以得出 K 是一域, 而 $\lambda \to \overline{\lambda}$ 是单位映射. 故当 K 不是域或 $\lambda \to \overline{\lambda}$ 不是 K 的单位映射时, 定理成立. 当 K 是域而 $\lambda \to \overline{\lambda}$ 又是 K 的单位映射时, 因 H 不是交错矩阵, 故 K 是特征数 $\neq 2$ 的域, 而 H 是对称矩阵, 即 $\rho=1$; 这时 $\lambda\rho\overline{a}+a\overline{\lambda}=2a\lambda \neq 0$ 对一切 $\lambda \neq 0$, 因此, 这时定理也成立.

利用定理 1, 我们可以解决特征数 $\neq 2$ 的代数封闭域上对称矩阵的合同问题.

定理 2　设 K 为特征数 $\neq 2$ 的代数封闭域. K 上 $n \times n$ 对称矩阵 S 必与以下形状的一个矩阵合同:

$$\begin{pmatrix} 1 & & & & & \\ & 1 & & & 0 & \\ & & \ddots & & & \\ & & & 1 & & \\ & & & & 0 & \\ & & & & & \ddots \\ 0 & & & & & & 0 \end{pmatrix},$$

(r 个 1, $n-r$ 个 0)

而 r 为 S 的秩. 因而, K 上两个 $n\times n$ 对称矩阵合同, 当且仅当它们有相同的秩.

【证】 依定理 1, 有 K 上 $n\times n$ 可逆矩阵 P 存在, 使

$$PSP'=\begin{pmatrix} \lambda_1 & & & & & & \\ & \lambda_2 & & & & 0 & \\ & & \ddots & & & & \\ & & & \lambda_r & & & \\ & & & & 0 & & \\ & 0 & & & & \ddots & \\ & & & & & & 0 \end{pmatrix}.$$

令

$$Q=\begin{pmatrix} \lambda_1^{-\frac{1}{2}} & & & & & & \\ & \lambda_2^{-\frac{1}{2}} & & & & 0 & \\ & & \ddots & & & & \\ & & & \lambda_r^{-\frac{1}{2}} & & & \\ & & & & 1 & & \\ & 0 & & & & \ddots & \\ & & & & & & 1 \end{pmatrix}.$$

其中 $\lambda_i^{-\frac{1}{2}}$ 表 λ_i 在 K 中任意一个平方根, 则

$$QPSP'Q'=\begin{pmatrix} 1 & & & & & \\ & 1 & & & 0 & \\ & & \ddots & & & \\ & & & 1 & & \\ & & & & 0 & \\ & 0 & & & & \ddots \\ & & & & & & 0 \end{pmatrix}.$$

(r 个 1)

有趣的是定理 1 也解决了实四元数体上斜哈矩阵的合同问题.

定理 3 设 K 为实四元数体, $a\to\overline{a}$ 为 K 中共轭. K 上 $n\times n$ 斜哈矩阵 H 必与以下形状的一个矩阵合同:

$$\begin{pmatrix} i & & & & & \\ & i & & & 0 & \\ & & \ddots & & & \\ & & & i & & \\ & & & & 0 & \\ & 0 & & & & \ddots \\ & & & & & & 0 \end{pmatrix},$$

(前 r 个对角元为 i)

其中 $\bar{i}=-i, i^2=-1$, 而 r 为 H 的秩. 因而, K 上两个 $n\times n$ 斜哈矩阵合同, 当且仅当它们有相同的秩.

【证】 依定理 1, 有 K 上 $n\times n$ 可逆矩阵 P 存在, 使

$$PH\overline{P}'=\begin{pmatrix} \lambda_1 & & & & & \\ & \lambda_2 & & & 0 & \\ & & \ddots & & & \\ & & & \lambda_r & & \\ & & & & 0 & \\ & 0 & & & & \ddots \\ & & & & & & 0 \end{pmatrix},$$

$\overline{\lambda}_j=-\lambda_j\neq 0$. 对于每个 j, 可以写 $\lambda_j=N(\lambda_j)^{\frac{1}{2}}\dfrac{\lambda_j}{N(\lambda_j)^{\frac{1}{2}}}$. 于是

$$N\left(\frac{\lambda_j}{N(\lambda_j)^{\frac{1}{2}}}\right)=1,$$

$$T\left(\frac{\lambda_j}{N(\lambda_j)^{\frac{1}{2}}}\right)=0,$$

因而有 $q_j\in K$, 使 $q_j\dfrac{\lambda_j}{N(\lambda_j)^{\frac{1}{2}}}\overline{q}_j=i\ (j=1,\cdots,r)$. 令

$$Q=\begin{pmatrix} q_1N(\lambda_1)^{-\frac{1}{4}} & & & & & & \\ & q_2N(\lambda_2)^{-\frac{1}{4}} & & & 0 & & \\ & & \ddots & & & & \\ & & & q_rN(\lambda_r)^{-\frac{1}{4}} & & & \\ & & & & 1 & & \\ & 0 & & & & \ddots & \\ & & & & & & 1 \end{pmatrix},$$

则 $QPH\overline{P}'\overline{Q}'$ 即为所求形状的矩阵.

在 §4, 我们会看到对于 K 上哈矩阵并无相应结果.

现在设 $K=F_q$ 为 q 个元素的有限域, 以 F_q^* 表 F_q 的乘法群, 以 F_q^{*2} 表 F_q^* 中平方元素组成的群. 我们知道, F_q^* 为循环群, 设 z 是它的一个生成元. 如果 K 的

特征数 $=2$, 则 $F_q^{*2}=F_q^*$. 如果 K 的特征数 $\neq 2$, 则 $F_q^*:F_q^{*2}=2$. 现在先设 F_q 的特征数 $\neq 2$, 这时 $z\notin F_q^{*2}$, 而 F_q^* 中任一非平方元素皆可表作 $zy^2, y^2\in F_q^{*2}$.

定理 4 设 S 为特征数 $\neq 2$ 的域 F_q 上的 $n\times n$ 可逆对称矩阵, 则必合同于以下形状的一个矩阵:

$$\begin{pmatrix} 1 & & & 0 \\ & \ddots & & \\ & & 1 & \\ 0 & & & s \end{pmatrix},$$

其中 $s=1$ 或 z. 因此, F_q 上 $n\times n$ 可逆对称矩阵在合同下分成两类, 一类的判别式属于 F_q^{*2}, 另一类的判别式属于 zF_q^{*2}.

【证】 依定理 1, 有 F_q 上 $n\times n$ 可逆矩阵存在, 使

$$PSP'=\begin{pmatrix} \lambda_1 & & 0 \\ & \ddots & \\ 0 & & \lambda_n \end{pmatrix},$$

将 $\lambda_1,\cdots,\lambda_n$ 重排后, 可设 $\lambda_1,\cdots,\lambda_r\in F_q^{*2}$, 而 $\lambda_{r+1},\cdots,\lambda_n\notin F_q^{*2}$.

令

$$Q=\begin{pmatrix} \lambda_1^{-\frac12} & & & & & 0 \\ & \lambda_2^{-\frac12} & & & & \\ & & \ddots & & & \\ & & & \lambda_r^{-\frac12} & & \\ & & & & (z\lambda_{r+1}^{-1})^{\frac12} & \\ 0 & & & & & \ddots \\ & & & & & (z\lambda_n^{-1})^{\frac12} \end{pmatrix},$$

则

$$QPSP'Q'=\begin{pmatrix} 1 & & & & 0 \\ & \ddots & & & \\ & & 1 & & \\ & & & z & \\ 0 & & & & \ddots \\ & & & & & z \end{pmatrix}.$$

(其中 1 共 r 个.)

先设 $-1\notin F_q^{*2}$, 则当 x 跑过 F_q 时, $1+x^2$ 跑过 F_q^* 中 $\dfrac{q+1}{2}$ 个元素. 因而有 $x\in F_q^*$,

使 $1+x^2$ 为 F_q^* 中非平方元素. 设 $1+x^2=zy^2$, 则 $\begin{pmatrix} y^{-1} & y^{-1}x \\ -y^{-1}x & y^{-1} \end{pmatrix}$ 可逆, 而

$$\begin{pmatrix} y^{-1} & y^{-1}x \\ -y^{-1}x & y^{-1} \end{pmatrix}^{-1}\begin{pmatrix} z & 0 \\ 0 & z \end{pmatrix}\begin{pmatrix} y^{-1} & y^{-1}x \\ -y^{-1}x & y^{-1} \end{pmatrix}^{-1'}=\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}.$$

再设 $-1\in F_q^{*2}$, 令 $-1=x^2$, 则 $\begin{pmatrix} x & 1 \\ (2xz)^{-1} & (2xz)^{-1}x \end{pmatrix}$ 可逆, 而

$$\begin{pmatrix} x & 1 \\ (2xz)^{-1} & (2xz)^{-1}x \end{pmatrix}\begin{pmatrix} z & 0 \\ 0 & z \end{pmatrix}\begin{pmatrix} x & 1 \\ (2xz)^{-1} & (2xz)^{-1}x \end{pmatrix}'=\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}.$$

同样有

$$\begin{pmatrix} x & 1 \\ (2x)^{-1} & (2x)^{-1}x \end{pmatrix}\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}\begin{pmatrix} x & 1 \\ (2x)^{-1} & (2x)^{-1}x \end{pmatrix}'=\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}.$$

因此 $\begin{pmatrix} z & 0 \\ 0 & z \end{pmatrix}$ 和 $\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$ 合同. 这样就证明了本定理.

现在设 $K_0=F_q$ 是 q 个元素的有限域, 而 $K=F_{q^2}$ 为 F_q 的一个二次扩张域. 设 $a\to\overline{a}$ 是 K 的自同构 $a\to\overline{a}=a^q$. 于是我们有

定理 5 K 上 $n\times n$ 可逆 Hermite 矩阵皆与单位矩阵合同.

【证】 设 H 为 K 上 $n\times n$ 可逆 Hermite 矩阵. 依定理 1, 有 K 上 $n\times n$ 可逆矩阵 P, 使

$$PH\overline{P}'=\begin{pmatrix} \lambda_1 & & 0 \\ & \ddots & \\ 0 & & \lambda_n \end{pmatrix},$$

$\overline{\lambda}_i=\lambda_i\neq 0(i=1,\cdots,n)$. 于是 $\lambda_i\in F_q^*$. 如果 F_q 的特征数为 2, 则每个 λ_i 都是 F_q 中平方元素. 令

$$Q=\begin{pmatrix} \lambda_1^{-\frac{1}{2}} & & 0 \\ & \ddots & \\ 0 & & \lambda_n^{-\frac{1}{2}} \end{pmatrix},$$

则 $QPH\overline{P}'\overline{Q}'=I$. 如 F_q 的特征数 $\neq 2$, 我们先证明对于每个 $\lambda\in F_q^*$, 都有一个 $\mu\in F_{q^2}^*$, 使 $\mu\overline{\mu}=\lambda$. 实际上, 设 $\mu\in F_{q^2}^*$, 则 $\mu\to\mu\overline{\mu}$ 是从 $F_{q^2}^*$ 到 F_q^* 之中的一个同态映射, 问题是要证明, 它是映上的. 如 $\mu\overline{\mu}=1$, 则 $\mu^{q+1}=1$, 于是这个同态的核是 $F_{q^2}^*$ 的一个 $q+1$ 阶的子群, 因而这个同态的像是 F_q^* 的 $\dfrac{q^2-1}{q+1}=q-1$ 阶的子群, 因而

是 F_q^* 本身, 所以这个同态是映上的. 现在令 $\mu_i \in F_{q^2}^*$, 而 $\mu_i\overline{\mu}_i = \lambda_i (i = 1, 2, \cdots, n)$, 令

$$Q_1 = \begin{pmatrix} \mu_1^{-1} & & 0 \\ & \ddots & \\ 0 & & \mu_n^{-1} \end{pmatrix},$$

则 $Q_1PH\overline{P}'\overline{Q}_1' = I$.

定理 6 如 k 是 $K = F_{q^2}^*$ 中一个斜对称元素, 则 K 上 $n \times n$ 可逆斜 Hermite 矩阵皆与 kI 合同.

【证】 如 H 为 K 上斜 Hermite 矩阵, 则 $k^{-1}H$ 为 Hermite 矩阵. 于是有 K 上 $n \times n$ 可逆矩阵 P, 使 $Pk^{-1}H\overline{P}' = I$, 因之 $PH\overline{P}' = kI$.

定理 1 可作如下的推广, 这个推广以后经常被采用.

定理 7 设 K 是具对合 $a \to \overline{a}$ 的体, 而 H 是 K 上 $n \times n$ 哈矩阵或斜哈矩阵. (如 K 的特征数 $= 2$, H 不一定是迹式的.) 但假设 H 不是交错矩阵, 则 H 一定和一个对角形矩阵合同.

【证】 如果 H 是迹式的, 根据定理 1, H 一定和一个对角形矩阵合同.

检查一下定理 1 的证明, 就会发现, 这个证明对于特征数 =2 的体上的非迹式哈矩阵 H 也能适用, 只要 H 不是特征数 $= 2$ 的域上的对称矩阵.

我们只需要研究 H 是特征数 $= 2$ 的域 K 上的对称矩阵的情形. 根据假设, H 不是交错矩阵, 故 H 有非 0 对角线元素, 不妨设 H 的 (1, 1) 位置元素 $\neq 0$. 于是在 §2(1) 中取 $r = 1$, 就有 H 合同于

$$\begin{pmatrix} a_1 & 0 \\ 0 & H_1 \end{pmatrix},$$

其中 H_1 为 $(n-1) \times (n-1)$ 对称阵. 如 H_1 仍有非 0 对角元素, 重复上面讨论, H 就合同于

$$\begin{pmatrix} a_1 & & & & \\ & a_2 & & & 0 \\ & & \ddots & & \\ & & & a_r & \\ & 0 & & & H_r \end{pmatrix},$$

其中 H_r 为 $(n-r) \times (n-r)$ 对称阵, 而其对角线元素皆 0, 因此, 依定理 2.1, H_r 合同于

$$\begin{pmatrix} 0 & 1 & & & & & & \\ 1 & 0 & & & & & & \\ & & \ddots & & & & & \\ & & & 0 & 1 & & & \\ & & & 1 & 0 & & & \\ & & & & & 0 & & \\ & & & & & & \ddots & \\ & & & & & & & 0 \end{pmatrix}.$$

于是 H 合同于

$$\begin{pmatrix} a_1 & & & & & & & & & \\ & \ddots & & & & & & & & \\ & & a_r & & & & & & & \\ & & & 0 & 1 & & & & & \\ & & & 1 & 0 & & & & & \\ & & & & & \ddots & & & & \\ & & & & & & 0 & 1 & & \\ & & & & & & 1 & 0 & & \\ & & & & & & & & 0 & \\ & & & & & & & & & \ddots \\ & & & & & & & & & & 0 \end{pmatrix}.$$

如能证明

$$\begin{pmatrix} a & & \\ & 0 & 1 \\ & 1 & 0 \end{pmatrix} \quad (a \neq 0)$$

与对角矩阵合同, 即可知 H 与对角矩阵合同. 实际上,

$$\begin{pmatrix} 1 & 0 & a \\ 1 & 1 & 0 \\ a^{-1} & a^{-1} & 1 \end{pmatrix} \begin{pmatrix} a & & \\ & 0 & 1 \\ & 1 & 0 \end{pmatrix} \begin{pmatrix} 1 & 0 & a \\ 1 & 1 & 0 \\ a^{-1} & a^{-1} & 1 \end{pmatrix}' = \begin{pmatrix} a & 0 & 0 \\ 0 & a & 0 \\ 0 & 0 & a^{-1} \end{pmatrix}.$$

因此定理 7 成立.

§4　H- 矩阵在合同下的化简 (续)——Witt 定理

为了更进一步讨论 H- 矩阵的合同, 我们将证明

定理 1　(Witt 定理)　设可逆 H- 矩阵

$$\begin{pmatrix} H & 0 \\ 0 & H_1 \end{pmatrix}, \quad \begin{pmatrix} H & 0 \\ 0 & H_2 \end{pmatrix}$$

合同, 则 H_1 和 H_2 合同.

【证】　如所讨论的 H- 矩阵是交错矩阵, 那么本定理是 §2 定理 1, 系理 1 的直接推论. 因此, 只需要讨论 H- 矩阵不是交错矩阵的情形, 这时不妨假设我们讨论的 H- 矩阵为迹式哈矩阵. 依 §3 定理 1, 我们更可设 H 是对角形矩阵. 用归纳法向 H 的级数, 可将定理化归为以下特例的证明：从

$$\begin{pmatrix} h & 0 \\ 0 & H_1 \end{pmatrix}, \begin{pmatrix} h & 0 \\ 0 & H_2 \end{pmatrix} \quad (h \in K,\ \overline{h} = \rho h, h \neq 0)$$

合同推出 H_1 和 H_2 合同.

设

$$\begin{pmatrix} a & u \\ \nu' & D \end{pmatrix}\begin{pmatrix} h & 0 \\ 0 & H_1 \end{pmatrix}\begin{pmatrix} \overline{a} & \overline{v} \\ \overline{u}' & \overline{D}' \end{pmatrix} = \begin{pmatrix} h & 0 \\ 0 & H_2 \end{pmatrix},$$

则

$$\begin{aligned} ah\overline{a} + uH_1\overline{u}' &= h, \\ ah\overline{v} + uH_1\overline{D}' &= 0, \\ v'h\overline{a} + DH_1\overline{u}' &= 0, \\ v'h\overline{v} + DH_1\overline{D}' &= H_2. \end{aligned}$$

设 $\lambda \in K$, 则

$$\begin{aligned} &(v'\lambda u + D)H_1\overline{(v'\lambda u + D)}' \\ &= v'(\lambda h\overline{\lambda} - \lambda ah\overline{a}\overline{\lambda} - \lambda ah - h\overline{a}\overline{\lambda} - h)\overline{v} + H_2. \end{aligned}$$

如 $a \neq 1$, 令 $\lambda = (1-a)^{-1}$, 则

$$\begin{aligned} &\lambda h\overline{\lambda} - \lambda ah\overline{a}\overline{\lambda} - \lambda ah - h\overline{a}\overline{\lambda} - h \\ &= (1-a)^{-1}[h - ah\overline{a} - ah(1-\overline{a}) - (1-a)h\overline{a}](1-\overline{a})^{-1} - h \\ &= (1-a)^{-1}[h - ah - h\overline{a} + ah\overline{a}](1-\overline{a})^{-1} - h = 0, \end{aligned}$$

于是

$$(v'(1-a)^{-1}u + D)H_1\overline{(v'(1-a)^{-1}u + D)}' = H_2.$$

如 $a = 1$, 因所讨论的是迹式哈矩阵, 可写 $h = h_1 + \overline{h}_1$, 而 $h_1 \in K$. 这时令 $\lambda = -h_1h^{-1}$, 则

$$\begin{aligned} &\lambda h\overline{\lambda} - \lambda ah\overline{a}\overline{\lambda} - \lambda ah - h\overline{a}\overline{\lambda} - h \\ &= \lambda h\overline{\lambda} - \lambda h\overline{\lambda} - \lambda h - h\overline{\lambda} - h \\ &= h_1h^{-1}h + hh^{-1}\overline{h}_1 - h \\ &= h_1 + \overline{h}_1 - h = 0, \end{aligned}$$

于是

$$(-v'h_1h^{-1}u + D)H_1\overline{(-v'h_1h^{-1}u + D)}' = H_2.$$

无论在哪种情形都有 H_1 和 H_2 合同.

利用 Witt 定理, 我们可以解决实数域上对称矩阵的合同问题及复数域上 Hermite 矩阵的合同问题.

定理 2　设 S 为实系数 $n\times n$ 对称矩阵, 则 S 合同于 $n\times n$ 矩阵

$$\begin{pmatrix} \underbrace{\begin{matrix}1 & & \\ & \ddots & \\ & & 1\end{matrix}}_{p} & & & & & \\ & \underbrace{\begin{matrix}-1 & & \\ & \ddots & \\ & & -1\end{matrix}}_{q} & & \\ & & 0 & & \\ & & & \ddots & \\ & & & & 0 \end{pmatrix},$$

其中 $p+q=r$ 是 S 的秩. 更进一步, p,q 由 S 唯一确定, 我们把 $p-q$ 称为 S 的符号差.

【证】　依定理 3.1 有实系数 $n\times n$ 可逆矩阵 P 存在, 使

$$PSP'=\begin{pmatrix} \lambda_1 & & & & & \\ & \ddots & & & & \\ & & \lambda_r & & & \\ & & & 0 & & \\ & & & & \ddots & \\ & & & & & 0 \end{pmatrix}.$$

不妨设 $\lambda_1,\cdots,\lambda_p>0$, 而 $\lambda_{p+1},\cdots,\lambda_r<0$. 令

$$Q=\begin{pmatrix} \lambda_1^{-\frac{1}{2}} & & & & & & & \\ & \ddots & & & & & & \\ & & \lambda_p^{-\frac{1}{2}} & & & & & \\ & & & (-\lambda_{p+1})^{-\frac{1}{2}} & & & & \\ & & & & \ddots & & & \\ & & & & & (-\lambda_r)^{-\frac{1}{2}} & & \\ & & & & & & 1 & \\ & & & & & & & \ddots \\ & & & & & & & & 1 \end{pmatrix},$$

则 $QPSP'Q'$ 即为所求形状的矩阵.

其次, 设

$$\begin{pmatrix} \underbrace{1 \ddots 1}_{p} & & & \\ & \underbrace{-1 \ddots -1}_{q} & & \\ & & 0 & \\ & & & \ddots & \\ & & & & 0 \end{pmatrix} \text{与} \begin{pmatrix} \underbrace{1 \ddots 1}_{p'} & & & \\ & \underbrace{-1 \ddots -1}_{q'} & & \\ & & 0 & \\ & & & \ddots & \\ & & & & 0 \end{pmatrix}$$

合同, 其中 $p+q=p'+q'=r$, 即

$$\begin{pmatrix} A^{(r)} & B \\ C & D^{(n-r)} \end{pmatrix} \left(\begin{array}{cc|c} \underbrace{1 \ddots 1}_{p} & & 0 \\ & \underbrace{-1 \ddots -1}_{q} & \\ \hline \multicolumn{2}{c|}{0} & \begin{matrix} 0 & & \\ & \ddots & \\ & & 0 \end{matrix} \end{array}\right) \begin{pmatrix} A^{(r)} & B \\ C & D^{(n-r)} \end{pmatrix}'$$

$$= \begin{pmatrix} \underbrace{1 \ddots 1}_{p'} & & & \\ & \underbrace{-1 \ddots -1}_{q'} & & \\ & & 0 & \\ & & & \ddots & \\ & & & & 0 \end{pmatrix}.$$

由此推出

$$A \begin{pmatrix} \underbrace{1 \ddots 1}_{p} & 0 \\ 0 & \underbrace{-1 \ddots -1}_{q} \end{pmatrix} A' = \begin{pmatrix} \underbrace{1 \ddots 1}_{p'} & 0 \\ 0 & \underbrace{-1 \ddots -1}_{q'} \end{pmatrix}.$$

因之

$$\begin{pmatrix} \underbrace{\begin{matrix}1 & & \\ & \ddots & \\ & & 1\end{matrix}}_{p} & 0 \\ 0 & \underbrace{\begin{matrix}-1 & & \\ & \ddots & \\ & & -1\end{matrix}}_{q} \end{pmatrix} \text{和} \begin{pmatrix} \underbrace{\begin{matrix}1 & & \\ & \ddots & \\ & & 1\end{matrix}}_{p'} & 0 \\ 0 & \underbrace{\begin{matrix}-1 & & \\ & \ddots & \\ & & -1\end{matrix}}_{q'} \end{pmatrix}$$

合同. 如 $p > p'$, 则依 Witt 定理,

$$\begin{pmatrix} \underbrace{\begin{matrix}1 & & \\ & \ddots & \\ & & 1\end{matrix}}_{p-p'} & 0 \\ 0 & \underbrace{\begin{matrix}-1 & & \\ & \ddots & \\ & & -1\end{matrix}}_{q} \end{pmatrix} \text{与} \begin{pmatrix} -1 & & 0 \\ & \ddots & \\ 0 & & -1 \end{pmatrix}_{q'}$$

合同, 即有 $q' \times q'$ 可逆矩阵 L 使

$$\begin{pmatrix} \underbrace{\begin{matrix}1 & & \\ & \ddots & \\ & & 1\end{matrix}}_{p-p'} & 0 \\ 0 & \underbrace{\begin{matrix}-1 & & \\ & \ddots & \\ & & -1\end{matrix}}_{q} \end{pmatrix} = L \begin{pmatrix} \underbrace{\begin{matrix}-1 & & \\ & \ddots & \\ & & -1\end{matrix}}_{q'} \end{pmatrix} L',$$

以 $l_{11}, l_{12}, \cdots, l_{1q'}$ 表 L 的第一行中诸元素, 比较上式 (1, 1) 位置元素得

$$1 = -(l_{11}^2 + l_{12}^2 + \cdots + l_{1q'}^2).$$

因 $l_{11}, \cdots, l_{1q'}$ 皆实数, 此为不可能. 同样可证 $p < p'$ 亦不可能. 因此 $p = p', q = q'$.
同理可证

定理 3　设 H 为复系数的 $n \times n$ Hermite 矩阵, 则 H 合同于 $n \times n$ 矩阵

$$\begin{pmatrix} \underbrace{\begin{matrix}1 & & \\ & \ddots & \\ & & 1\end{matrix}}_{p} & & 0 \\ & \underbrace{\begin{matrix}-1 & & \\ & \ddots & \\ & & -1\end{matrix}}_{q} & \\ 0 & & \begin{matrix}0 & & \\ & \ddots & \\ & & 0\end{matrix} \end{pmatrix},$$

其中 $p + q = r$ 是 H 的秩. 更进一步, p, q 由 H 唯一确定; 我们把 $p - q$ 称为 H 的符号差.

由定理 3 立刻推出

定理 4 设 H 为复系数的 $n\times n$ 斜 Hermite 矩阵. 则 H 合同于 $n\times n$ 矩阵

$$\begin{pmatrix} \underbrace{\begin{matrix} i & & \\ & \ddots & \\ & & i \end{matrix}}_{p} & & & 0 \\ & \underbrace{\begin{matrix} -i & & \\ & \ddots & \\ & & -i \end{matrix}}_{q} & & \\ & & \begin{matrix} 0 & & \\ & \ddots & \\ & & 0 \end{matrix} \\ 0 & & & \end{pmatrix},$$

其中 $p+q=r$ 是 H 的秩. 更进一步 p,q 由 H 唯一确定; 我们把 $p-q$ 称为 H 的符号差.

像定理 2 一样可证

定理 5 设 H 是实四元数体上的 $n\times n$ Hamilton 矩阵, 则 H 合同于 $n\times n$ 矩阵

$$\begin{pmatrix} \underbrace{\begin{matrix} 1 & & \\ & \ddots & \\ & & 1 \end{matrix}}_{p} & & & 0 \\ & \underbrace{\begin{matrix} -1 & & \\ & \ddots & \\ & & -1 \end{matrix}}_{q} & & \\ & & \begin{matrix} 0 & & \\ & \ddots & \\ & & 0 \end{matrix} \\ 0 & & & \end{pmatrix},$$

其中 $p+q=r$ 是 H 的秩. 更进一步, p,q 由 H 唯一确定, 我们把 $p-q$ 称为 H 的符号差.

与定理 3.3 相比较, 可见实四元数体上 Hamilton 与斜 Hamilton 矩阵的理论很不一样.

§5 迷向子空间

除非另有声明, 以下我们永远假定在我们所讨论的有对合的体 K 中选定了一个对合 $a\to\bar{a}$, 而且选定了 K 上的一个对这个对合而言的 $n\times n$ 可逆 H- 矩阵 H.

定义 1 设 P 是一个 $r\times n$ 矩阵, 其 r 行线性无关. 由 P 的 r 行生成的子空

间为简单起见仍以 P 表之. 我们按照

$$PH\overline{P}'$$

是可逆, 不可逆或零矩阵分别称 P 为非迷向, 迷向或全迷向子空间.

显然, 一维迷向子空间一定是全迷向的, 我们称之为迷向线, 它里面任意一个非零向量称为迷向向量. 如 H 为交错矩阵, 则任一向量皆迷向.

定理 1　任一迷向子空间中必含有迷向线.

【证】　设 P 是 $r\times n$ 矩阵, 而 $PH\overline{P}'$ 是不可逆的. 则存在一个 r 维非零向量 x, 使 $xPH\overline{P}'=0$, 因之

$$xPH\overline{P}'\overline{x}'=0,$$

这表明 xP 是含在迷向子空间 P 中的迷向线.

定义 2　设 P 为一子空间, 一切适合条件

$$PH\overline{x}'=0$$

的 n 维向量 x 组成一个向量子空间, 称为 P 的共轭子空间, 以 P^* 表之. 如 P 是 r 维的, 易见 P^* 是 $n-r$ 维的.

定理 2　子空间 P 是迷向子空间, 当且仅当 $P\cap P^*\neq 0$, 而 P 是全迷向子空间, 当且仅当 $P\subseteq P^*$.

【证】　(i) 设 P 是 r 维迷向子空间, 则 $H_1=PH\overline{P}'$ 是不可逆的. 即有一 r 维向量 $x\neq 0$, 使 $H_1\overline{x}'=0$. 故 $PH\overline{P}'\overline{x}'=0$, 即 $xP\in P^*$. 显然 $xP\in P$, 故 $xP\in P\cap P^*$. 反之, 若 $P\cap P^*\neq 0$, 则有一 n 维非零向量 $y\in P\cap P^*$. 由 $y\in P^*$, 可得 $PH\overline{y}'=0$. 因 $y\in P$, 有 r 维向量 x 使 $y=xP$. 于是 $PH\overline{y}'=PH\overline{P}'\overline{x}'=0$, 即 $PH\overline{P}'$ 不是可逆的.

(ii) 定理之第二部分乃显而易见. 因为 $PH\overline{P}'=0$ 的必要且充分条件是 $P\subseteq P^*$.

定理 3　若 P 是非迷向子空间, 则 P^* 也是非迷向的, 而且 $(P^*)^*=P$.

【证】　若 $PH\overline{P}'$ 可逆, 而 $P^*H\overline{P^*}'$ 非可逆, 则

$$\begin{pmatrix} P \\ P^* \end{pmatrix} H \overline{\begin{pmatrix} P \\ P^* \end{pmatrix}}' = \begin{pmatrix} PH\overline{P}' & 0 \\ 0 & P^*H\overline{P^*}' \end{pmatrix}$$

是不可逆的. 因 H 是可逆的, 故 $P\cap P^*\neq 0$. 由定理 2, 此与 P 的非迷向性相矛盾.

定理 3　H 的极大全迷向子空间是一全迷向子空间, 它不再包在更大的全迷向子空间内.

由此定义立刻推出, H 的任一全迷向子空间一定包含在一个极大全迷向子空间之内.

定理 4 一 H- 矩阵 H 若无迷向线, 则称为定号的, 即由

$$xH\overline{x}' = 0$$

推出 $x = 0$. 不然称为不定号的.

显然定号 H- 矩阵是可逆的, 且定号性质经合同关系而仍然保留.

我们举出下面这些例子来.

【例 1】 设 K 为域, H 为可逆交错矩阵. 这时, 每一个向量都是迷向向量, 因此交错矩阵不可能定号.

【例 2】 设 K 为代数封闭域, 其特征数 $\neq 2$, H 为 K 上 $n \times n$ 可逆对称矩阵, 则当 $n > 1$ 时, H 不可能定号. 实际上, 可设

$$H = \begin{pmatrix} 1 & & & 0 \\ & 1 & & \\ & & \ddots & \\ 0 & & & 1 \end{pmatrix}.$$

令 i 为 -1 在 K 中的一个根, 则 $(1, i, 0, \cdots, 0)$ 就是一个迷向向量.

【例 3】 设 H 为实数域上的 $n \times n$ 可逆对称矩阵或复数域上的 $n \times n$ 可逆 Hermite 矩阵, 则 H 是定号的, 当且仅当它的符号差为 $\pm n$.

【例 4】 在以实数域为基域的四元数体上, 任一可逆斜哈矩阵都不是定号的. 实际上, 依定理 3.3, 任一可逆 2×2 斜哈矩阵皆合同于

$$\begin{pmatrix} j & 0 \\ 0 & j \end{pmatrix}.$$

因 j 与 $-j$ 有相同的范与迹, 故有四元数 q 使

$$qj\overline{q} = -j.$$

则 $(q, 1)$ 就是一条迷向线.

【例 5】 若基域是有理数域, 四元数体的斜哈矩阵不一定常是非定号. 例如

$$\begin{pmatrix} i+j & 0 \\ 0 & i+j+k \end{pmatrix}$$

是一斜哈方阵, 但此乃定号的. 其理由是: 若有一四元数 q, 使

$$q(i+j)\overline{q} = -(i+j+k),$$

则得出

$$2N(q)^2 = 3,$$

而 $\frac{3}{2}$ 非有理数的平方.

【例 6】 设 $K = F_q$, 而 K 的特征数 $\neq 2$, 则 F_q 上 2×2 对称矩阵

$$S_1 = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$$

是定号的, 当且仅当 $-1 \notin F_q^{*2}$, 而 2×2 对称矩阵

$$S_2 = \begin{pmatrix} 1 & 0 \\ 0 & z \end{pmatrix}$$

是定号的, 当且仅当 $-1 \in F_q^{*2}$. 实际上, 如 (a, b) 是 S_1 的一个迷向向量, 则 $a^2 + b^2 = 0$. 由此推出 $-1 \in F_q^{*2}$. 反之, 如 $-1 = y^2 \in F_q^{*2}$, 则 $(1, y)$ 是 S_1 的一个迷向向量. 其次, 如 (c, d) 是 S_2 的一个迷向向量, 则 $c^2 + d^2 z = 0$, 由此推出 $-z \in F_q^{*2}$, 因之 $-1 \notin F_q^{*2}$. 反之, 如 $-1 \notin F_q^{*2}$, 则 $-z \in F_q^{*2}$, 写 $-z = y^2$, 则 $(y, 1)$ 就是 S_2 的一个迷向向量.

【例 7】 设 $K_0 = F_q$, 而 $K = K_{q^2}, K$ 有二阶自同构 $a \to \overline{a} = a^q$. K 上 2×2 Hermite 矩阵皆不定号. 实际上, 只要证

$$\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$$

不定号即可. 依定理 3.5 的证明, 有 $\mu \in K$, 使 $\mu\overline{\mu} = -1$, 即 $(1, \mu)$ 就是一条迷向线.

定理 4 若可逆 H- 矩阵 H 有一 ν 维极大全迷向子空间, 则 H 合同于如下形状的矩阵:

$$\begin{pmatrix} 0 & I^{(\nu)} & 0 \\ \rho I^{(\nu)} & 0 & 0 \\ 0 & 0 & \varDelta^{(n-2\nu)} \end{pmatrix},$$

此处 $\varDelta$ 是一定号对角形矩阵. 因之, 极大全迷向子空间的维数 ν 满足 $2\nu \leqslant n$.

【证】 令 P 为 H 的 ν 维极大全迷向子空间. 有一 $(n - \nu) \times n$ 矩阵 Q 存在, 使 $\begin{pmatrix} P \\ Q \end{pmatrix}$ 可逆. 于是

$$\begin{pmatrix} P \\ Q \end{pmatrix} H \overline{\begin{pmatrix} P \\ Q \end{pmatrix}}' = \begin{pmatrix} 0^{(\nu)} & L \\ \rho\overline{L}' & H_1 \end{pmatrix},$$

此处 $L=PH\overline{Q}'$ 之秩是 ν, 而 $H_1=QH\overline{Q}'$ 仍为 H- 矩阵. 故有二可逆矩阵 $A=A^{(\nu)}, B=B^{(n-\nu)}$ 使 $ALB=(I^{(\nu)}\ 0^{(\nu,n-2\nu)})$, 于是

$$\begin{pmatrix} A & 0 \\ 0 & \overline{B}' \end{pmatrix}\begin{pmatrix} 0 & L \\ \rho\overline{L}' & H_1 \end{pmatrix}\overline{\begin{pmatrix} A & 0 \\ 0 & \overline{B}' \end{pmatrix}}' = \begin{pmatrix} 0 & I^{(\nu)} & 0 \\ \rho I^{(\nu)} & H_2 & M \\ 0 & \rho\overline{M}' & H_3 \end{pmatrix},$$

其中 H_2, H_3 皆 H- 矩阵. 可以设

$$H_2=\begin{pmatrix} h_{11}+\rho\overline{h}_{11} & h_{12} & \cdots & h_{1\nu} \\ \rho\overline{h}_{12} & h_{22}+\rho\overline{h}_{22} & \cdots & h_{2\nu} \\ \vdots & & \ddots & \vdots \\ \rho\overline{h}_{1\nu} & \cdots\cdots & & h_{\nu\nu}+\rho\overline{h}_{\nu\nu} \end{pmatrix}.$$

当 H 是斜哈矩阵时, 这是显然的, 当 H 是哈矩阵时, 这是根据 H 的迹性. 命

$$T_2=\begin{pmatrix} h_{11} & h_{12} & \cdots & h_{1\nu} \\ 0 & h_{22} & \cdots & h_{2\nu} \\ \vdots & & \ddots & \vdots \\ 0 & \cdots & & h_{\nu\nu} \end{pmatrix}.$$

则

$$H_2=T_2+\rho\overline{T}_2'.$$

又

$$\begin{pmatrix} I & 0 & 0 \\ -T_2 & I & 0 \\ -\rho\overline{M}' & 0 & I \end{pmatrix}\begin{pmatrix} 0 & I & 0 \\ \rho I & H_2 & M \\ 0 & \rho\overline{M}' & H_3 \end{pmatrix}\overline{\begin{pmatrix} I & 0 & 0 \\ -T_2 & I & 0 \\ -\rho\overline{M}' & 0 & I \end{pmatrix}}' = \begin{pmatrix} 0 & I & 0 \\ \rho I & 0 & 0 \\ 0 & 0 & H_3 \end{pmatrix}.$$

由定理 3.1 可知有一可逆方阵 $R^{(n-2\nu)}$, 使 $RH_3\overline{R}'=\varDelta$ 是一对角形方阵. 因此我们有

$$\begin{pmatrix} I & 0 & 0 \\ 0 & I & 0 \\ 0 & 0 & R \end{pmatrix}\begin{pmatrix} 0 & I & 0 \\ \rho I & 0 & 0 \\ 0 & 0 & H_3 \end{pmatrix}\overline{\begin{pmatrix} I & 0 & 0 \\ 0 & I & 0 \\ 0 & 0 & R \end{pmatrix}}' = \begin{pmatrix} 0 & I^{(\nu)} & 0 \\ \rho I^{(\nu)} & 0 & 0 \\ 0 & 0 & \varDelta \end{pmatrix}.$$

最后还需要证明 $\varDelta$ 是定号的. 如 $\varDelta$ 不是定号的, 则有 $(n-2\nu)$ 维向量 x, 使 $x\varDelta\overline{x}'=0$. 于是

$$\begin{pmatrix} I^{(\nu)} & 0^{(\nu)} & 0^{(\nu,n-2\nu)} \\ 0 & 0 & x \end{pmatrix}$$

就是

$$\begin{pmatrix} 0 & I^{(v)} & 0 \\ \rho I^{(v)} & 0 & 0 \\ 0 & 0 & \Delta \end{pmatrix}$$

的一个全迷向子空间, 因之

$$\begin{pmatrix} I^{(\nu)} & 0 & 0 \\ 0 & 0 & x \end{pmatrix}\begin{pmatrix} I^{(\nu)} & 0 & 0 \\ 0 & I^{(\nu)} & 0 \\ 0 & 0 & R \end{pmatrix}\begin{pmatrix} I^{(\nu)} & 0 & 0 \\ -T_2 & I^{(\nu)} & 0 \\ -\rho\overline{M}' & 0 & I \end{pmatrix}\begin{pmatrix} A^{(\nu)} & 0 \\ 0 & \overline{B}' \end{pmatrix}\begin{pmatrix} P \\ Q \end{pmatrix}$$

就是 H 的一个全迷向子空间, 它的维数是 $\nu+1$, 而它包有 P, 这与 P 是极大全迷向子空间相抵触.

定理 5 H 的所有极大全迷向子空间的维数相同.

【证】 假定 H 有两个极大全迷向子空间, 其维数各为 ν_1 及 ν_2, 由定理 4, H 合同于

$$\begin{pmatrix} 0 & I^{(\nu_1)} & 0 \\ \rho I^{(\nu_1)} & 0 & 0 \\ 0 & 0 & \Delta_1 \end{pmatrix} \text{及} \begin{pmatrix} 0 & I^{(\nu_2)} & 0 \\ \rho I^{(\nu_2)} & 0 & 0 \\ 0 & 0 & \Delta_2 \end{pmatrix}.$$

假定 $\nu_1 \geqslant \nu_2$. 则由 Witt 定理, 可知 Δ_2 与

$$\begin{pmatrix} 0 & I^{(\nu_1-\nu_2)} & 0 \\ \rho I^{(\nu_1-\nu_2)} & 0 & 0 \\ 0 & 0 & \Delta_1 \end{pmatrix}$$

合同. 因为 Δ_2 是定号的, 所以 $\nu_1-\nu_2=0$. 因此 $\nu_1=\nu_2$.

定义 5 一可逆 H- 矩阵 H 的极大全迷向子空间的维数称为此方阵的指数.

定理 6 两个可逆 H- 矩阵合同的必要且充分条件是: 它们的指数相同, 而且它们的定号部分合同.

基于定理 4 和定理 5, 再根据以前的讨论, 我们有以下诸结果:

I. 设 K 为域, K 上 $n\times n$ 可逆交错矩阵 H 的指数 $\nu=\dfrac{n}{2}$(因 H 可逆, 故 n 一定是偶数), 而 H 一定合同于

$$\begin{pmatrix} 0 & I^{(\nu)} \\ -I^{(\nu)} & 0 \end{pmatrix}.$$

II. 设 K 为特征数 $\neq 2$ 的代数封闭域, 则 K 上 $n\times n$ 可逆对称矩阵 H 的指数

$\nu=\left[\dfrac{n}{2}\right]$, 而 H 一定合同于

$$\begin{pmatrix} 0 & I^{(\nu)} \\ I^{(\nu)} & 0 \end{pmatrix} \quad 或 \quad \begin{pmatrix} 0 & I^{(\nu)} & 0 \\ I^{(\nu)} & 0 & 0 \\ 0 & 0 & 1 \end{pmatrix},$$

依 n 为偶数或奇数而定.

III. 设 K 为实数域 (或复数域, 实四元数体), 则 K 上 $n\times n$ 可逆对称矩阵 (或 Hermite 矩阵, 哈矩阵)H 的指数 $v=\min(p,n-p)$, 而 H 一定合同于

$$\begin{pmatrix} 0 & I^{(\nu)} & 0 \\ I^{(\nu)} & 0 & 0 \\ 0 & 0 & I^{(n-2\nu)} \end{pmatrix} \quad 或 \quad \begin{pmatrix} 0 & I^{(\nu)} & 0 \\ I^{(\nu)} & 0 & 0 \\ 0 & 0 & -I^{(n-2\nu)} \end{pmatrix},$$

依 $p\geqslant n-p$ 或 $p\leqslant n-p$ 而定.

IV. 设 K 为实四元数体, 则 K 上 $n\times n$ 斜哈矩阵 H 的指数 $\nu=\left[\dfrac{n}{2}\right]$, 而 H 一定合同于

$$\begin{pmatrix} 0 & I^{(\nu)} \\ -I^{(\nu)} & 0 \end{pmatrix} \quad 或 \quad \begin{pmatrix} 0 & I^{(\nu)} & 0 \\ -I^{(\nu)} & 0 & 0 \\ 0 & 0 & j \end{pmatrix},$$

依 n 为偶数或奇数而定.

V. 设 $K=F_q$ 为特征数 $\neq 2$ 的域. 如 n 为奇数, 则 K 上 $n\times n$ 对称矩阵的指数 $\nu=\left[\dfrac{n}{2}\right]=\dfrac{n-1}{2}$, 而 H 一定合同于

$$\begin{pmatrix} 0 & I^{(\nu)} & 0 \\ I^{(\nu)} & 0 & 0 \\ 0 & 0 & 1 \end{pmatrix} \quad 或 \quad \begin{pmatrix} 0 & I^{(\nu)} & 0 \\ I^{(\nu)} & 0 & 0 \\ 0 & 0 & z \end{pmatrix},$$

依 $(-1)^\nu\det H\in F_q^{*2}$ 或 $\notin F_q^{*2}$ 而定. 如 n 为偶数, 则 K 上 $n\times n$ 对称矩阵的指数 $\nu=\dfrac{n}{2}$ 或 $\dfrac{n}{2}-1$. 如 H 的指数 $\nu=\dfrac{n}{2}$, 则 H 一定合同于

$$\begin{pmatrix} 0 & I^{(\nu)} \\ I^{(\nu)} & 0 \end{pmatrix};$$

如 H 的指数 $\nu=\dfrac{n}{2}-1$, 则 H 一定合同于

$$\begin{pmatrix} \begin{matrix} 0 & I^{(\nu)} \\ I^{(\nu)} & 0 \end{matrix} & 0 \\ 0 & \begin{pmatrix} 1 & 0 \\ 0 & q \end{pmatrix} \end{pmatrix},$$

其中 $q=1$ 或 z 视 $-1\notin F_q^{*2}$ 或 $-1\in F_q^{*2}$ 而定.

VI. 设 $K_0=F_q$, 而 $K=F_{q^2}$, 则 K 上 $n\times n$ 可逆 Hermite 矩阵 H 的指数 $\nu=\left[\frac{n}{2}\right]$, 而 H 一定合同于

$$\begin{pmatrix} 0 & I^{(\nu)} \\ I^{(\nu)} & 0 \end{pmatrix} \quad 或 \quad \begin{pmatrix} 0 & I^{(\nu)} & 0 \\ I^{(\nu)} & 0 & 0 \\ 0 & 0 & 1 \end{pmatrix},$$

依 n 为偶数或奇数而定.

最后, 我们证明

定理 7　命 P 是一 p 维的向量子空间, 且 $PH\overline{P}'$ 的秩是 r. 于是有一 $p\times p$ 可逆矩阵 Q 及一 $(n-p)\times n$ 的矩阵 Z, 使

$$\begin{pmatrix} QP \\ Z \end{pmatrix} H \overline{\begin{pmatrix} QP \\ Z \end{pmatrix}}' = \begin{pmatrix} H_1^{(r)} & 0 & 0 & 0 \\ 0 & 0 & I^{(p-r)} & 0 \\ 0 & \rho I^{(p-r)} & 0 & 0 \\ 0 & 0 & 0 & H_2 \end{pmatrix},$$

其中 H_1 及 H_2 都是可逆的.

【证】　由定理 1.1, 有一 $p\times p$ 可逆方阵 Q_1, 使

$$Q_1(PH\overline{P}')\overline{Q_1}' = \begin{pmatrix} H_1^{(r)} & 0 \\ 0 & 0 \end{pmatrix},$$

此处 H_1 是可逆 H- 矩阵. 有一 $(n-p)\times n$ 矩阵 R, 使

$$\begin{pmatrix} Q_1P \\ R \end{pmatrix} H \overline{\begin{pmatrix} Q_1P \\ R \end{pmatrix}}' = \begin{pmatrix} H_1^{(r)} & 0^{(r,p-r)} & M_1^{(r,n-p)} \\ 0 & 0^{(p-r)} & M_2 \\ \rho\overline{M_1}' & \rho\overline{M_2}' & H_3 \end{pmatrix}.$$

于是

$$\begin{pmatrix} I^{(r)} & 0 & 0 \\ 0 & I^{(p-r)} & 0 \\ -\rho\overline{M_1}'H_1^{-1} & 0 & I \end{pmatrix} \begin{pmatrix} H_1^{(r)} & 0 & M_1 \\ 0 & 0 & M_2 \\ \rho\overline{M_1}' & \rho\overline{M_2}' & H_3 \end{pmatrix} \overline{\begin{pmatrix} I^{(r)} & 0 & 0 \\ 0 & I^{(p-r)} & 0 \\ -\rho\overline{M_1}'H_1^{-1} & 0 & I \end{pmatrix}}'$$
$$= \begin{pmatrix} H_1^{(r)} & 0 & 0 \\ 0 & 0 & M_2 \\ 0 & \rho\overline{M_2}' & H_4 \end{pmatrix}.$$

依定理 4 的证明, 存在一可逆 $(n-r)$ 行矩阵 L, 其形式是

$$L=\begin{pmatrix} L_{11}^{(p-r)} & 0^{(p-r,n-p)} \\ L_{21} & L_{22}^{(n-p)} \end{pmatrix},$$

使

$$L\begin{pmatrix} 0 & M_2 \\ \rho\overline{M_2}' & H_4 \end{pmatrix}\overline{L}'=\begin{pmatrix} 0 & I^{(p-r)} & 0 \\ \rho I^{(p-r)} & 0 & 0 \\ 0 & 0 & H_2 \end{pmatrix}.$$

方阵

$$\begin{pmatrix} I^{(r)} & 0^{(r,p-r)} & 0 \\ 0 & L_{11}^{(p-r)} & 0 \\ 0 & L_{21} & L_{22} \end{pmatrix}\begin{pmatrix} I^{(r)} & 0 & 0 \\ 0 & I^{(p-r)} & 0 \\ -\rho\overline{M_1}'H_1^{-1} & 0 & I \end{pmatrix}\begin{pmatrix} Q_1P \\ R \end{pmatrix}$$

适合定理所要求的条件. 故定理得证.

§6 酉 群

在本节中我们仍假定 K 为体, $a\to\overline{a}$ 为 K 的一个对合, 而 H 为 K 上 $n\times n$ 可逆 H- 矩阵. K 上一个 $n\times n$ 矩阵 U 称为酉矩阵, 或确切地, 对 H 而言的酉矩阵, 如果

$$UH\overline{U}'=H.$$

显而易见, K 上对 H 而言的酉矩阵的全体组成一群, 记作 $U_n(K,H)$, 称为 K 上对 H 而言的 n 级酉群. H 的指数亦称为 $U_n(K,H)$ 的指数. 如 K 为域, 而 H 为 K 上交错矩阵, 则 $U_n(K,H)$ 称为辛群, 记作 $Sp_n(K,H)$. 如 K 为域, 其特征数 $\neq 2$, 而 H 为 K 上对称矩阵, 则 $U_n(K,H)$ 称为正交群, 记作 $O_n(K,H)$. 如 K 为复数域, $a\to\overline{a}$ 是 K 中共轭, 而 $H=I$, 则 $U_n(K,I)$ 就是通常的酉群.

我们先给出以下几个注意:

I. 如 H_1 和 H_2 是两个合同的可逆 H- 矩阵, 则 $U_n(K,H_1)$ 和 $U_n(K,H_2)$ 同构. 设 $PH_1\overline{P}'=H_2$. 如 $U\in U_n(K,H)$, 即 $UH_1\overline{U}'=H_1$, 则 $PUP^{-1}\in U_n(K,H_2)$; 实际上,

$$\begin{aligned}(PUP^{-1})H_2\overline{(PUP^{-1})}'&=PUP^{-1}H_2\overline{P^{-1}}'\overline{U}'\overline{P}'\\ &=PUH_1\overline{U}'\overline{P}'=PH_1\overline{P}'=H_2.\end{aligned}$$

而且

$$U\to PUP^{-1}$$

是从 $U_n(K,H_1)$ 到 $U_n(K,H_2)$ 之上的一个同构映射. 因此 $U_n(K,H_1)$ 与 $U_n(K,H_2)$ 同构. 根据定理 5.4, K 上 $n\times n$ 可逆 H- 矩阵合同于形状

$$\begin{pmatrix} 0 & I^{(\nu)} & 0 \\ \rho I^{(\nu)} & 0 & 0 \\ 0 & 0 & \Delta^{(n-2\nu)} \end{pmatrix}$$

的 H- 矩阵, 其中 ν 为指数, Δ 为定号对角形 H- 矩阵, 因此只需讨论这种形状的 H- 矩阵所定义的酉群即可.

特别, 因域 K 上任意两个同级的可逆交错矩阵皆合同, 因此对于一个给定的级数 $n=2m$, 实质上只有一个辛群, 我们把它记作 $Sp_n(K)$, 并把它看作是

$$\begin{pmatrix} 0 & I^{(m)} \\ -I^{(m)} & 0 \end{pmatrix}$$

所定义的辛群. 又因有限域 $K=F_{q^2}$ 上任意两个可逆 Hermite 矩阵皆等价, 因此对于一个给定的级数 n, 实际只有一个酉群, 我们把它记作 $U_n(F_{q^2})$, 可把它看作单位矩阵定义的酉群, 亦可看作由

$$\begin{pmatrix} 0 & I^{(\nu)} \\ I^{(\nu)} & 0 \end{pmatrix} \text{或} \begin{pmatrix} 0 & I^{(\nu)} & 0 \\ I^{(\nu)} & 0 & 0 \\ 0 & 0 & 1 \end{pmatrix},$$

其中 $\nu=\left[\dfrac{n}{2}\right]$, 所定义的酉群.

II. 如 H 为 K 上 $n\times n$ 可逆哈矩阵, $\lambda\neq 0$ 为 K 的对称元素, 而且 λ 属于 K 的中心 Z, 则 $U_n(K,H)$ 和 $U_n(K,\lambda H)$ 完全相重.

特别, 如 $K=F_q$, 而 K 的特征数 $\neq 2$, 对于一个给定的级数 $n=2m+1$, 实质上只有一个正交群. 我们知道 F_q 上一个可逆对称矩阵必合同于

$$H_1=\begin{pmatrix} 0 & I^{(m)} & 0 \\ I^{(m)} & 0 & 0 \\ 0 & 0 & 1 \end{pmatrix} \quad \text{或} \quad H_2=\begin{pmatrix} 0 & I^{(m)} & 0 \\ I^{(m)} & 0 & 0 \\ 0 & 0 & z \end{pmatrix}.$$

但 $O_n(F_q,H_2)=O_n(F_q,zH_2)$, 而 zH_2 又与 H_1 合同, 因之 $O_n(F_q,H_2)$ 与 $O_n(F_q,H_1)$ 同构. 因此我们只需要研究由 H_1 所定义的正交群. 至于当 $n=2m$ 为偶数, F_q 上一个可逆对称矩阵必合同于

$$\begin{pmatrix} 0 & I^{(m)} \\ I^{(m)} & 0 \end{pmatrix} \quad \text{或} \quad \begin{pmatrix} 0 & I^{(m-1)} & 0 \\ I^{(m-1)} & 0 & 0 \\ 0 & & \begin{pmatrix} 1 & 0 \\ 0 & q \end{pmatrix} \end{pmatrix},$$

其中 $\begin{pmatrix} 1 & 0 \\ 0 & q \end{pmatrix}$ 定号. 这时我们需要考虑两个同一级数的正交群.

III. 设 K 的特征数 $\neq 2$, H 为 K 上 H- 矩阵, 其标元为 ρ. 设 α 为 K 中斜对称元素, 即 $\overline{\alpha} = -\alpha$, 则 $H_1 = \alpha^{-1}H$ 为 K 上对于对合 $a \to \widetilde{a} = \alpha^{-1}\overline{a}\alpha$ 的 H- 矩阵, 而其标元为 $-\rho$. 我们有 $U_n(K,H)$ 与 $U_n(K,H_1)$ 同构.

如 $U \in U_n(K,H)$, 即 $UH\overline{U}' = H$, 则 $\alpha^{-1}U\alpha \in U_n(K,H_1)$; 实际上, $\alpha^{-1}U\alpha H_1 \cdot \widetilde{\alpha^{-1}U\alpha}' = \alpha^{-1}U\alpha\alpha^{-1}H\overline{U}' = \alpha^{-1}UH\overline{U}' = \alpha^{-1}H = H_1$. 而且

$$U \to \alpha^{-1}U\alpha$$

为从 $U_n(K,H)$ 到 $U_n(K,H_1)$ 之上的一个同构. 因此 $U_n(K,H)$ 与 $U_n(K,H_1)$ 同构. 这表明只要 K 中有斜对称元素, 即 $a \to \overline{a}$ 不是单位自同构, 哈矩阵所定义的酉群的研究可化归为斜哈矩阵所定义的酉群的研究, 而且反之亦然.

更进一步我们注意, 如 P 为 H 的极大全迷向子空间, 则 $\alpha^{-1}P\alpha$ 为 H_1 的极大全迷向子空间. 实际上,

$$\alpha^{-1}P\alpha H_1\widetilde{\alpha^{-1}P\alpha}' = \alpha^{-1}P\alpha\alpha^{-1}H\overline{P}' = \alpha^{-1}PH\overline{P}' = 0,$$

因此 H_1 与 H 有相同的指数. 这表明当我们将哈矩阵 (或斜哈矩阵) 所定义的酉群的研究化归斜哈矩阵 (或哈矩阵) 所定义的酉群的研究时, 它们的指数一定相同.

在以下讨论中我们固定一个酉群 $U_n(K,H)$.

定义 1　两个 p 维子空间各以 $p\times n$ 矩阵 X 和 Y 表之. X 和 Y 称为酉等价, 或确切地说, 在 $U_n(K,H)$ 下等价, 如有一 $p\times p$ 可逆矩阵 Q 和一矩阵 $U \in U_n(K,H)$, 使

$$X = QYU. \tag{1}$$

定理 1　两个 p 维子空间 X 和 Y 酉等价, 当且仅当 $XH\overline{X}'$ 和 $YH\overline{Y}'$ 合同.

【证】　(i) 由 (1) 式可知,

$$XH\overline{X}' = QYUH\overline{U}'\overline{Y}'\overline{Q}' = Q(YH\overline{Y}')\overline{Q}',$$

即 $XH\overline{X}'$ 及 $YH\overline{Y}'$ 合同.

(ii) 反之, 假定 $XH\overline{X}'$ 与 $YH\overline{Y}'$ 合同, 其秩必相同, 命之为 r. 由定理 5.7, 可知有两个可逆的 p 行 p 列方阵 Q 及 Q_1 存在, 及有两个 $n-p$ 行 n 列矩阵 Z, Z_1 存在, 使

$$\begin{pmatrix} QX \\ Z \end{pmatrix} H \overline{\begin{pmatrix} QX \\ Z \end{pmatrix}}' = \begin{pmatrix} H_1^{(r)} & 0 & 0 & 0 \\ 0 & 0 & I^{(p-r)} & 0 \\ 0 & \rho I^{(p-r)} & 0 & 0 \\ 0 & 0 & 0 & H_2 \end{pmatrix}$$

及

$$\begin{pmatrix} Q_1Y \\ Z_1 \end{pmatrix} H \overline{\begin{pmatrix} Q_1Y \\ Z_1 \end{pmatrix}}' = \begin{pmatrix} H_1^{(r)} & 0 & 0 & 0 \\ 0 & 0 & I^{(p-r)} & 0 \\ 0 & \rho I^{(p-r)} & 0 & 0 \\ 0 & 0 & 0 & H_3 \end{pmatrix},$$

此处 H_1, H_2, H_3 是可逆的 H- 矩阵. 由 Witt 定理, 知 H_2 与 H_3 合同, 即有一 L, 使

$$H_2 = LH_3\overline{L}'.$$

故

$$\begin{pmatrix} I & 0 \\ 0 & L \end{pmatrix}\begin{pmatrix} Q_1Y \\ Z_1 \end{pmatrix} H \overline{\begin{pmatrix} Q_1Y \\ Z_1 \end{pmatrix}}' \overline{\begin{pmatrix} 1 & 0 \\ 0 & L \end{pmatrix}}' = \begin{pmatrix} H_1^{(r)} & 0 & 0 & 0 \\ 0 & 0 & I^{(p-r)} & 0 \\ 0 & \rho I^{(p-r)} & 0 & 0 \\ 0 & 0 & 0 & H_2 \end{pmatrix}.$$

记

$$\begin{pmatrix} I & 0 \\ 0 & L \end{pmatrix}\begin{pmatrix} Q_1Y \\ Z_1 \end{pmatrix} = \begin{pmatrix} Q_1Y \\ Z_2 \end{pmatrix}.$$

如此则

$$\begin{pmatrix} Q_1Y \\ Z_2 \end{pmatrix} H \overline{\begin{pmatrix} Q_1Y \\ Z_2 \end{pmatrix}}' = \begin{pmatrix} QX \\ Z \end{pmatrix} H \overline{\begin{pmatrix} QX \\ Z \end{pmatrix}}'.$$

命

$$U = \begin{pmatrix} Q_1Y \\ Z_2 \end{pmatrix}^{-1} \begin{pmatrix} QX \\ Z \end{pmatrix},$$

显然 $U \in U_n(K,H)$. 由此得出 $X = Q^{-1}Q_1YU$.

系理 1　同维的全迷向子空间一定酉等价. 特别, 极大全迷向子空间皆酉等价.

系理 2　设 X 和 Y 是两个 p 秩的 $p\times n$ 矩阵, 那么 $U_n(K,H)$ 中有一元素 U 存在, 使 $X = YU$ 的充要条件为 $XH\overline{X}' = YH\overline{Y}'$.

只要仔细检查一下定理 1 的证明, 即可发现本系理成立.

最后, 我们给出酉群的一个子群. $U_n(K,H)$ 中行列式为 $1(K^*/C$ 的单位元) 的元素组成一群, 记作 $U_n^+(K,H)$. 特别, 我们有 $O_n^+(K,H)$, 这里 K 为特征数 $\neq 2$ 的域而 H 为 K 上 $n\times n$ 可逆对称矩阵. 但需注意 $Sp_{2v}^+(K) = Sp_{2v}(K)$, 这是定理 2.3 的系理.

§7 当 $\nu=\dfrac{n}{2}$ 时酉矩阵的形式

设 H 是体 K 上指数 $\nu=\frac{1}{2}n$ (n 一定是偶数) 的 H- 矩阵. 不失普遍性, 我们可以假定

$$H=\begin{pmatrix}0 & I\\ \rho I & 0\end{pmatrix}\quad(\rho=\pm 1).$$

命 U 表 $U_n(K,H)$ 中之一元素, 把 U 写成

$$U=\begin{pmatrix}A & B\\ C & D\end{pmatrix}, A=A^{(v)}, B=B^{(v)}\text{等等}.$$

由 $UH\overline{U}'=H$ 可以得出

$$\begin{aligned}&A\overline{B}'+\rho B\overline{A}'=0,\quad C\overline{D}'+\rho D\overline{C}'=0,\\ &A\overline{D}'+\rho B\overline{C}'=I.\end{aligned}$$

求 $UH\overline{U}'=H$ 之逆. 由 $H^{-1}=\rho H$, 可得 $\overline{U}'HU=H$. 故若 U 是对 H 的酉矩阵, 则 $\overline{U}'$ 亦然. 由此立刻得出

$$\begin{aligned}&\overline{A}'C+\rho\overline{C}'A=0,\quad \overline{B}'D+\rho\overline{D}'B=0,\\ &\overline{A}'D+\rho\overline{C}'B=I.\end{aligned}$$

我们可以举出以下若干有用的酉方阵:

I. $\begin{pmatrix}A & 0\\ 0 & \overline{A}'^{-1}\end{pmatrix}$, 其中 A 是 $\nu\times\nu$ 可逆矩阵, 即 $A\in GL_\nu(K)$.

II. 平移

$$\begin{pmatrix}I^{(\nu)} & Q\\ 0 & I^{(\nu)}\end{pmatrix},$$

此处 Q 是 $\nu\times\nu$ 矩阵, 满足 $\overline{Q}'=-\rho Q$.

III. 拟对合

$$\begin{pmatrix}J & I^{(\nu)}-J\\ \rho(I^{(\nu)}-J) & J\end{pmatrix},$$

此处 J 是 $\nu\times\nu$ 对角线方阵, 适合于 $J^2=J$.

先引进以下定义:

定义 1 一对 $\nu\times\nu$ 矩阵 (X,Y) 如适合以下条件, 则称为一 H- 对:

(i) 如果把 (X,Y) 看成是一个 ν 行 2ν 列的矩阵, 则其秩为 ν;

(ii) $(X\ Y)\begin{pmatrix} 0 & I \\ \rho I & 0 \end{pmatrix}\overline{(X\ Y)}'=(0)$,

即 $X\overline{Y}'=-\rho Y\overline{X}'$.

显然, 酉变换

$$(X_1\ Y_1)=Q(X\ Y)U \quad (U\in U_n(K,H))$$

变 H- 对为 H- 对. 又若

$$\begin{pmatrix} A & B \\ C & D \end{pmatrix}$$

在 $U_n(K,H)$ 之中, 则 $(A\ B)$ 成一 H- 对, $(C\ D)$ 亦复如是. 又可见一极大全迷向子空间可由一 H- 对代表, 且其逆亦真. 又若 X 是可逆的, 则 $X^{-1}Y$ 是标元为 $-\rho$ 的 H- 矩阵.

定理 1　对任一 H- 对 (X,Y), 我们有拟对合 Σ 使

$$(X\ Y)=(X^*\ Y^*)\Sigma,$$

其中 X^* 是可逆的.

【证】　若 X 本身是可逆的, 取 $\Sigma=I$ 即可. 今假定 X 是不可逆的, 则有一可逆矩阵 P 及一置换矩阵 Q, 使

$$X_1=PXQ=\begin{pmatrix} H_1 & H_2 \\ 0 & 0 \end{pmatrix},$$

此处 $H_1=H_1^{(r)}$ 是可逆的. 命

$$Y_1=PY\overline{Q}'^{-1},$$

则

$$(X_1\ Y_1)=P(X\ Y)\begin{pmatrix} Q & 0 \\ 0 & \overline{Q}'^{-1} \end{pmatrix}.$$

写

$$Y_1=\begin{pmatrix} T_1^{(r)} & T_2 \\ T_3 & T_4 \end{pmatrix}.$$

因为 (X,Y) 是 H- 对, 故 (X_1,Y_1) 亦然. 于是由

$$\begin{pmatrix} H_1 & H_2 \\ 0 & 0 \end{pmatrix}\overline{\begin{pmatrix} T_1 & T_2 \\ T_3 & T_4 \end{pmatrix}}'=\begin{pmatrix} * & H_1\overline{T_3}'+H_2\overline{T_4}' \\ 0 & 0 \end{pmatrix}$$

得出

$$H_1\overline{T_3}'+H_2\overline{T_4}'=0,$$

即

$$T_3=-T_4\overline{H_2}'\overline{H_1}'^{-1}.$$

因为

$$(X_1,Y_1)=\left(\begin{pmatrix} H_1 & H_2 \\ 0 & 0 \end{pmatrix},\begin{pmatrix} T_1 & T_2 \\ -T_4\overline{H_2}'\overline{H_1}'^{-1} & T_4 \end{pmatrix}\right)$$

的秩是 ν, 故 T_4 是可逆的. 命

$$J=\begin{pmatrix} 0 & 0 \\ 0 & I^{(\nu-r)} \end{pmatrix},$$

则得

$$\left(\begin{pmatrix} H_1 & H_2 \\ 0 & 0 \end{pmatrix},\begin{pmatrix} T_1 & T_2 \\ -T_4\overline{H_2}'\overline{H_1}'^{-1} & T_4 \end{pmatrix}\right)\begin{pmatrix} I-J & J \\ \rho J & I-J \end{pmatrix}$$
$$=\left(\begin{pmatrix} H_1 & \rho T_2 \\ 0 & \rho T_4 \end{pmatrix},*\right)=(X_2,Y_2),$$

此处 X_2 是可逆的. 因为 Q 是置换矩阵, 令

$$\Sigma=\begin{pmatrix} Q & 0 \\ 0 & \overline{Q}'^{-1} \end{pmatrix}\begin{pmatrix} I-J & J \\ \rho J & I-J \end{pmatrix}\begin{pmatrix} Q & 0 \\ 0 & \overline{Q}'^{-1} \end{pmatrix}^{-1},$$

则 Σ 是一拟对合. 再命

$$(X^*,Y^*)=P^{-1}(X_2,Y_2)\begin{pmatrix} Q & 0 \\ 0 & \overline{Q}'^{-1} \end{pmatrix}^{-1},$$

则 X^* 也是可逆的, 而

$$\begin{aligned}(X^*\ Y^*)&=P^{-1}(X_1,Y_1)\begin{pmatrix} I-J & J \\ \rho J & I-J \end{pmatrix}\begin{pmatrix} Q & 0 \\ 0 & \overline{Q}'^{-1} \end{pmatrix}^{-1}\\&=P^{-1}P(X\ Y)\begin{pmatrix} Q & 0 \\ 0 & \overline{Q}'^{-1} \end{pmatrix}\begin{pmatrix} I-J & J \\ \rho J & I-J \end{pmatrix}\begin{pmatrix} Q & 0 \\ 0 & \overline{Q}'^{-1} \end{pmatrix}^{-1}\\&=(X\ Y)\Sigma,\end{aligned}$$

定理于是得证.

由此定理立刻可以推出

定理 2 在群 $U_n(K,H)$ 之下, H- 对所代表的诸线性空间组成一可递集.

【证】 由定理 1, 任一 H- 对在 $U_n(K,H)$ 下可变为形如 (X,Y) 的 H- 对, 其中 X 是可逆的.

可是,

$$(X\ Y) = X(I\ X^{-1}Y) = X(I\ 0)\begin{pmatrix} I & S \\ 0 & I \end{pmatrix},$$

其中 $S = X^{-1}Y$ 是以 $-\rho$ 为标元的 H- 矩阵, 即

$$\begin{pmatrix} I & S \\ 0 & I \end{pmatrix}$$

属于酉群 $U_n(K,H)$. 故 $(X\ Y)$ 可经酉变换而变为 $(I\ 0)$.

【备注】 实际上, 定理 2 是定理 6.1 系理 2 的一个特例, 现在的证明则与前不同.

定理 3 对任一 H- 对 (X,Y), 必有一 H- 对 (U,V) 使

$$\begin{pmatrix} X & Y \\ U & V \end{pmatrix} \in U_n(K,H).$$

此定理由定理 2 可直接推出.

定理 4 在 $U_n(K,H)$ 中之任一方阵可以表成形状

(1) $$\begin{pmatrix} I & 0 \\ X & I \end{pmatrix}\begin{pmatrix} A & 0 \\ 0 & \overline{A}'^{-1} \end{pmatrix}\begin{pmatrix} I & Y \\ 0 & I \end{pmatrix}\Sigma,$$

其中 $A \in GL_\nu(K)$, X 及 Y 分别适合 $\overline{X}' = \rho X$ 及 $\overline{Y}' = -\rho Y$, 而 Σ 为一拟对合.

【证】 命

$$\begin{pmatrix} A & B \\ C & D \end{pmatrix}$$

是 $U_n(K,H)$ 中的一个元素. 由定理 1, 只需证明 A 是可逆的情况. 而如此, 则

$$\begin{pmatrix} A & B \\ C & D \end{pmatrix} = \begin{pmatrix} I & 0 \\ CA^{-1} & I \end{pmatrix}\begin{pmatrix} A & 0 \\ 0 & \overline{A}'^{-1} \end{pmatrix}\begin{pmatrix} I & A^{-1}B \\ 0 & I \end{pmatrix}.$$

显然, $A^{-1}B$ 及 CA^{-1} 是以 $-\rho$ 为标元的哈或斜哈矩阵. 定理证毕.

【附注】 (1) 式的表法不是唯一的.

定理 5 群 $U_n(K,H)$ 可由 I, II, III 三种元素生成.

【证】 因为

$$\begin{pmatrix} I & 0 \\ \rho Q & I \end{pmatrix} = \begin{pmatrix} 0 & I \\ \rho I & 0 \end{pmatrix}\begin{pmatrix} I & Q \\ 0 & I \end{pmatrix}\begin{pmatrix} 0 & I \\ \rho I & 0 \end{pmatrix}^{-1}.$$

定理 6 设 K 为域, 则 $Sp_{2\nu}(K)$ 中元素的行列式皆为 1.

【证】　这时 K 为域, $a\to\overline{a}$ 为单位映射, 而 $\rho=-1$. 于是 I, II, III 三种元素为

$$\begin{pmatrix} A & 0 \\ 0 & A'^{-1} \end{pmatrix},\quad \begin{pmatrix} I & Q \\ 0 & I \end{pmatrix},\quad \begin{pmatrix} 0 & I \\ -I & 0 \end{pmatrix},$$

其中 $|A|\neq 0, Q'=-Q$. 易见它们的行列式皆为 1, 因此本定理由定理 5 推出.

系理　设 K 为域, 则 $Sp_{2\nu}(K)\subseteq SL_{2\nu}(K)$. 而当 $\nu=1$ 时, 我们有 $Sp_2(K)=SL_2(K)$.

【证】　第一个结论是定理 6 的直接推论. 至于第二个断言, 因 $SL_2(K)$ 由 $B_{12}(\lambda)$ 及 $B_{21}(\mu)(\lambda,\mu\in K)$ 所生成, 而 $B_{12}(\lambda),B_{21}(\lambda)\in Sp_2(K)$, 故 $SL_2(K)\subseteq Sp_2(K)$. 因之 $Sp_2(K)=SL_2(K)$.

§8　当 $0<\nu<\frac{n}{2}$ 时酉矩阵的形式

今设 H 的指数 $\nu>0$. 不失普遍性, 可以取

$$H=\begin{pmatrix} 0 & I^{(\nu)} & 0 \\ \rho I^{(\nu)} & 0 & 0 \\ 0 & 0 & \varDelta \end{pmatrix},$$

此处 $\varDelta$ 是定号的. 极大全迷向子空间可以一 ν 行 n 列矩阵 $(X^{(\nu)}Y^{(\nu)}Z)$ 表之, 此矩阵之秩是 ν, 且适合等式

$$(X\ Y\ Z)H(\overline{X}\ \overline{Y}\ \overline{Z})'=0,$$

即 $X\overline{Y}'+\rho Y\overline{X}'+Z\varDelta\overline{Z}'=0$. 显然, 若

$$\begin{pmatrix} A & B & P \\ C & D & Q \\ R & T & U \end{pmatrix}$$

是 $U_n(K,H)$ 中的一元素, 则 $(A\ B\ P)$ 及 $(C\ D\ Q)$ 代表两个极大全迷向子空间.

显然, 下面一些矩阵是酉矩阵:

I.
$$\begin{pmatrix} \begin{matrix} A & B \\ C & D \end{matrix} & 0 \\ 0 & I \end{pmatrix},$$

此处 $\begin{pmatrix} A & B \\ C & D \end{pmatrix}\in U_{2\nu}(K,H_1)$, 而 $H_1=\begin{pmatrix} 0 & I^{(\nu)} \\ \rho I^{(\nu)} & 0 \end{pmatrix}$.

II.
$$\begin{pmatrix} I & & \\ & I & \\ & & U \end{pmatrix},$$

此处 $U \in U_{n-2\nu}(K, \Delta)$, 即 $U\Delta\overline{U}' = \Delta$.

III.
$$\begin{pmatrix} I & -\rho P\Delta_1\overline{P}' & P \\ 0 & I & 0 \\ 0 & -\rho\Delta_1\overline{P}' & I \end{pmatrix},$$

此处 $P = P^{(\nu,n-2\nu)}$, 而 Δ_1 为对角形矩阵且满足 $\Delta_1 + \rho\overline{\Delta}_1 = \Delta$. (当 K 的特征数 $\neq 2$ 时, 取 $\Delta_1 = \frac{1}{2}\Delta$ 即可, 而当 K 的特征数 $= 2$ 时, Δ_1 的存在由 H 的迹性所保证.)

我们亦称

$$\begin{pmatrix} J & I-J & 0 \\ \rho(I-J) & J & 0 \\ 0 & 0 & I \end{pmatrix}$$

为拟对合, 此处 J 是对角线方阵, 且 $J^2 = J$.

定理 1　若 $(X\ Y\ Z)$ 是一极大全迷向子空间, 则有一拟对合 Σ, 使

$$(X^*\ Y^*\ Z^*) = (X\ Y\ Z)\Sigma,$$

其中 X^* 是可逆的.

【证】　若 X 是可逆的, 则可取 $\Sigma = I$. 若 X 不是可逆的, 如定理 7.1 的证明, 有一可逆矩阵 P 及一置换矩阵 Q, 使

$$X_1 = PXQ = \begin{pmatrix} H_1 & H_2 \\ 0 & 0 \end{pmatrix},$$

此处 $H_1 = H_1^{(r)}$ 是可逆的. 命

$$Y_1 = PY\overline{Q}'^{-1} = \begin{pmatrix} T_1 & T_2 \\ T_3 & T_4 \end{pmatrix},\quad Z_1 = PZ = \begin{pmatrix} U_1 \\ U_2 \end{pmatrix},$$

则

$$(X_1\ Y_1\ Z_1) = P(X\ Y\ Z)\begin{pmatrix} Q & 0 & 0 \\ 0 & \overline{Q}'^{-1} & 0 \\ 0 & 0 & I \end{pmatrix}.$$

因为 $(X_1\ Y_1\ Z_1)$ 表一极大全迷向子空间, 所以

$$\begin{aligned}0&=X_1\overline{Y_1}'+\rho Y_1\overline{X_1}'+Z_1\Delta\overline{Z_1}'\\&=\begin{pmatrix}H_1&H_2\\0&0\end{pmatrix}\begin{pmatrix}\overline{T_1}'&\overline{T_3}'\\\overline{T_2}'&\overline{T_4}'\end{pmatrix}+\rho\begin{pmatrix}T_1&T_2\\T_3&T_4\end{pmatrix}\begin{pmatrix}\overline{H_1}'&0\\\overline{H_2}'&0\end{pmatrix}+\begin{pmatrix}U_1\\U_2\end{pmatrix}\Delta\begin{pmatrix}\overline{U_1}\\U_2\end{pmatrix}'\\&=\begin{pmatrix}H_1\overline{T_1}'+H_2\overline{T_2}'&H_1\overline{T_3}'+H_2\overline{T_4}'\\0&0\end{pmatrix}\\&\quad+\rho\begin{pmatrix}T_1\overline{H_1}'+T_2\overline{H_2}'&0\\T_3\overline{H_1}'+T_4\overline{H_2}'&0\end{pmatrix}+\begin{pmatrix}U_1\Delta\overline{U_1}'&U_1\Delta\overline{U_2}'\\U_2\Delta\overline{U_1}'&U_2\Delta\overline{U_2}'\end{pmatrix},\end{aligned}$$

由此得出 $U_2\Delta\overline{U_2}'=0$. 因为 Δ 是定号的, 所以 $U_2=0$. 又 $T_3\overline{H_1}'+T_4\overline{H_2}'=0$, 如定理 7.1 的证明, 可以完成本定理的证明.

由此可以立刻推出

定理 2 任一 $(X\ Y\ Z)$ 如代表一极大全迷向子空间, 则有一以 $(X\ Y\ Z)$ 为前 ν 行的酉矩阵

$$\begin{pmatrix}X&Y&Z\\A&B&C\\D&E&F\end{pmatrix}$$

存在.

定理 3 任一酉矩阵可以表成

$$\begin{pmatrix}I&0&0\\-X\Delta_1\overline{X}'&I&X\\-\Delta\overline{X}'&0&I\end{pmatrix}\begin{pmatrix}A&B&\\C&D&\\&&U\end{pmatrix}\begin{pmatrix}I&-\rho Y\Delta_1\overline{Y}'&Y\\0&I&0\\0&-\rho\Delta\overline{Y}'&I\end{pmatrix}\Sigma.$$

【证】 设

$$\begin{pmatrix}A&B&P\\C&D&Q\\R&T&U\end{pmatrix}$$

是一酉矩阵, 依定理 1, 只需证明 A 是可逆的情形. 取 $Y=-A^{-1}P, X=\overline{A}'^{-1}\overline{R}'\overline{\Delta}'^{-1}$, 则

$$\begin{aligned}&\begin{pmatrix}I&0&0\\-X\Delta_1\overline{X}'&I&X\\-\Delta\overline{X}'&0&I\end{pmatrix}\begin{pmatrix}A&B&P\\C&D&Q\\R&T&U\end{pmatrix}\begin{pmatrix}I&-\rho Y\Delta_1\overline{Y}'&Y\\0&I&0\\0&-\rho\Delta\overline{Y}'&I\end{pmatrix}\\&=\begin{pmatrix}A^*&B^*&0\\C^*&D^*&Q^*\\0&T^*&U^*\end{pmatrix},\end{aligned}$$

此处 $A^* = A$ 是可逆的. 因为这仍是个酉矩阵, 故 $Q^* = 0, T^* = 0$. 于是定理得证.

定理 4 酉群可由 I, II, III 三种元素生成之.

【证】 因为

$$\begin{pmatrix} 0 & I & \\ \rho I & 0 & \\ & & I \end{pmatrix}\begin{pmatrix} I & 0 & 0 \\ -X\Delta_1\overline{X}' & I & X \\ -\Delta\overline{X}' & 0 & I \end{pmatrix}\begin{pmatrix} 0 & \rho I & \\ I & 0 & \\ & & I \end{pmatrix} = \begin{pmatrix} I & -\rho X\Delta_1\overline{X}' & X \\ 0 & I & 0 \\ 0 & -\rho\Delta\overline{X}' & I \end{pmatrix},$$

所以由定理 3 推出本定理.

§9 酉平延及拟对称

设 A 和 B 是酉群 $U_n(K,H)$ 中的两个元素, 我们说它们酉相似, 如果存在一个 $U \in U_n(K,H)$, 使

$$A = U^{-1}BU.$$

我们不拟讨论一般的酉矩阵的酉相似问题, 而只准备讨论所谓酉原阵的酉相似问题.

酉矩阵 T 称为酉原阵, 如果 $T-I$ 的秩是 1, 换言之, 适合方程

$$xT = x$$

的 n 维向量组成一个 $n-1$ 维的子空间. 我们要寻求酉原阵酉相似的条件及在酉相似下的标准形.

设 T 是酉原阵, 因 $T-I$ 的秩为 1, 我们可以写

(1) $$T = I + \overline{u}'v,$$

而 u, v 是两个 n 维向量. 因 $T \in U_n(K,H)$, 我们有

(2) $$\overline{u}'vH + H\overline{v}'u + \overline{u}'vH\overline{v}'u = 0.$$

我们分别研究 v 是迷向向量及 v 不是迷向向量这两种情形.

先设 v 是迷向向量, 即 $vH\overline{v}' = 0$, 这时 T 称为酉平延. 于是 (2) 式成为

$$\overline{u}'vH + H\overline{v}'u = 0,$$

即

(3) $$(\overline{\overline{u}'vH})' = -\rho(\overline{u}'vH).$$

这表明 $\overline{u}'vH$ 是一个标元为 $-\rho$ 的哈或斜哈矩阵, 而且它的秩为 1. 如 K 为域, $a \to \overline{a}$ 为单位映射, 而 $\rho \neq -1$, 这样的矩阵不可能存在. 在其余情况, 依定理 3.7, 秩为 1 的哈或斜哈矩阵 $\overline{u}'vH$ 可表作

(4) $$\overline{u}'vH=\overline{x}'\mu x,$$
其中 x 为 n 维向量, 而 $\overline{\mu}=-\rho\mu$. 由 (4) 式推出
$$vH=\alpha\mu x,$$
而 $\alpha\in K$, 于是
$$u=\overline{\alpha}^{-1}x.$$
因此
$$vH=\alpha\mu\overline{\alpha}\mu.$$
令 $\lambda^{-1}=-\alpha\mu\overline{\alpha}$, 则 $\overline{\lambda}=-\rho\lambda$. 于是 $u=-\lambda vH$, 而 T 可表作

(5) $$T=I+H\overline{v}'\lambda v,$$
其中 $\overline{\lambda}=-\rho\lambda$.

是否 $\overline{\lambda}=-\rho\lambda$ 在 K 中恒有非零解呢? 如 $\rho=-1$, K 中非零对称元素皆为 $\overline{\lambda}=-\rho\lambda$ 的解. 当 $\rho\neq-1$ 时, $\overline{\lambda}=-\rho\lambda$ 在 K 中有非零解除非 $\overline{\lambda}=\lambda$, 对一切 $\lambda\in K$; 这时 K 为交换域. 因此, 除了 K 为域, $a\to\overline{a}$ 为单位自同构, $\rho\neq-1$ 这一情形外, 对任一迷向向量 v 及任一 K 中适合 $\overline{\lambda}=-\rho\lambda$ 的非零元素 λ, 矩阵 (5) 皆酉平延.

定理 1 设 $\nu\geqslant1$. 则除了 K 为域, $a\to\overline{a}$ 为单位映射而 $\rho\neq-1$ 这一情形外, 即除了 $U_n(K,H)$ 是正交群之外, $U_n(K,H)$ 中确有酉平延存在. 而 $U_n(K,H)$ 中酉平延皆可表作

(5) $$T=I+H\overline{v}'\lambda v,$$
其中 $vH\overline{v}'=0$, 而 $\overline{\lambda}=-\rho\lambda$.

系理 1 在定理 1 的假设下, 任一酉平延皆酉相似于以下形状的酉平延:

(6) $$I+\begin{pmatrix}0&0&0\\ [\lambda,0,\cdots,0]&0&0\\ 0&0&0\end{pmatrix}\quad(\overline{\lambda}=-\rho\lambda).$$

【证】 因任一迷向向量皆酉等价于 $(1,0,\cdots,0)$. 在 (5) 中取 $v=(1,0,\cdots,0)$ 即得形状 (6) 的矩阵.

系理 2 在定理 1 的假设下, 两个酉平延
$$T_1=I+H\overline{v_1}'\lambda_1v_1\ \text{及}\ T_2=I+H\overline{v_2}'\lambda_2v_2$$
酉相似, 当且仅当有 $a\in K$, 使 $\lambda_1=\overline{a}\lambda_2a$.

【证】 设 $U^{-1}T_1U=T_2$, 则
$$(\overline{v_1U})'\lambda_1(v_1U)=\overline{v_2}'\lambda_2v_2,$$
于是有 $a\in K$, 使 $v_1U=a^{-1}v_2$, 因之 $\lambda_1=\overline{a}\lambda_2a$.

反之, 设有 $a \in K$, 使 $\lambda_1 = \overline{a}\lambda_2 a$. 不妨设 T_1, T_2 的形状皆是 (6). 这时, 显然 T_1 与 T_2 酉相似.

其次, 我们研究酉原阵 $T = I + \overline{u}'v$ 中 v 为非迷向向量的情形, 这时 T 称为拟对称. 显然, 这时 H 不能是交错矩阵. 令

$$vH\overline{v}' = a, \quad v\overline{u}' = b.$$

将 (2) 式左乘以 v 后, 得到

$$bvH + au + bau = 0,$$

因 $b \neq -1$, 否则将有 $v = 0, T = I$, 于是

$$u = -a^{-1}(1+b)^{-1}bvH.$$

因之

$$b = v\overline{u}' = -vH\overline{v}'\overline{b}(1+\overline{b})^{-1}a^{-1} = -a\overline{b}(1+\overline{b})^{-1}a^{-1},$$

于是

(7) $$a\overline{b} + ba + ba\overline{b} = 0.$$

所以 T 可表作

(8) $$T = I - H\overline{v}'\overline{b}(1+\overline{b})^{-1}a^{-1}v = I + H\overline{v}'a^{-1}bv,$$

其中 $a = vH\overline{v}'$, 而 b 满足 (7) 式. 反之, 设 v 为非迷向向量, $a = vH\overline{v}'$, 而 b 满足 (7), 则 T 为拟对称.

是否 (7) 式恒有非零解呢? 实际上, 如果 K 的特征数 $\neq 2$, $b = -2$ 就是一个解. 当 $b = -2$ 时, 我们有

(8) $$T = I - 2H\overline{v}'a^{-1}v,$$

这时 $T^2 = I$. 我们把 (8) 称为对称, 它将一个 $n-1$ 维子空间中每个向量皆保持不变, 而将 v 映到 $-v$. 如果 K 的特征数为 2, 由 H 的迹性推出 $a = \lambda + \overline{\lambda}$, 而 $\lambda \in K, \overline{\lambda} \neq \lambda$; 这时 $b = \lambda\overline{\lambda}^{-1} + 1 \neq 0$ 即满足 (7). 因此, 除开辛群这一情形, $U_n(K, H)$ 恒有拟对称.

当 K 的特征数 $\neq 2, a \to \overline{a}$ 为单位自同构, 而 $\rho = 1$ 时, 正交群 $O_n(K, H)$ 中拟对称皆对称; 实际上, 这时 (7) 式只有 $b = -2$ 这一个非零解.

因此我们证明了

定理 2 除开辛群这一情形, $U_n(K, H)$ 中恒有拟对称, 而 $U_n(K, H)$ 中拟对称可表作

(8) $$T = I + H\overline{v}'(vH\overline{v}')^{-1}bv,$$

其中 v 为非迷向向量, 而 b 为满足 (7) 式的非零元素. 当 $U_n(K,H)$ 是特征数 $\neq 2$ 的域上正交群 $O_n(K,H)$ 时, 拟对称皆对称.

系理 1 设 $U_n(K,H)$ 不是辛群, $U_n(K,H)$ 中拟对称皆酉相似于以下形状的拟对称:

$$(9)\qquad \begin{pmatrix} 1+a^{-1}ba_1 & 0 & a^{-1}b & 0 & \\ 0 & I^{(\nu-1)} & 0 & 0 & \\ \rho\overline{a_1}a^{-1}ba_1 & 0 & 1+\rho\overline{a_1}a^{-1}b & 0 & \\ 0 & 0 & 0 & I^{(\nu-1)} & \\ & & & & I^{(n-2\nu)} \end{pmatrix},$$

其中 $\overline{a}=\rho a, a_1+\rho\overline{a_1}=a$, 而 b 为适合 (7) 的 K 中非零元素. 特别, 当 K 的特征数 $\neq 2$ 时, $U_n(K,H)$ 中对称皆酉相似于以下形状的拟对称:

$$(10)\qquad \begin{pmatrix} 0 & 0 & \lambda & 0 & \\ 0 & I^{(\nu-1)} & 0 & 0 & \\ \lambda^{-1} & 0 & 0 & 0 & \\ 0 & 0 & 0 & I^{(\nu-1)} & \\ & & & & I^{(n-2\nu)} \end{pmatrix},$$

其中 $\overline{\lambda}=\rho\lambda$.

【证】 先将 T 表成形状 (8). 令 $a=vH\overline{v}'$. 如 K 的特征数 $\neq 2$, 令 $a_1=\dfrac{1}{2}a$; 如 K 的特征数 $=2$, 由 H 的迹性有 a_1 存在, 使 $a_1+\overline{a}_1=a$. 因此无论在哪一种情形都有 $a_1+\rho\overline{a}_1=a$. 令

$$u=(a_1,\underbrace{0,\cdots,0}_{\nu-1},1,\underbrace{0,\cdots,0}_{\nu-1},\underbrace{0,\cdots,0}_{n-2\nu}).$$

注意 $uH\overline{u}'=a$, 因此依定理 6.1 有 $U\in U_n(K,H)$, 使 $vU=u$. 于是 $U^{-1}TU$ 即为形状 (9). 在 (9) 中令 $b=-2$, 即得 (10).

最后我们给出某些交换性的定理.

定理 3 设 $U_n(K,H)$ 包有酉平延

$$T=I+H\overline{v}'\lambda v,$$

如 $U_n(K,H)$ 中一个元素 U 与 T 交换, 则 vU 与 v 线性相关, 即 U 将迷向线 v 保持不变.

【证】 设 $UT=TU$, 则

$$UH\overline{v}'\lambda v=H\overline{v}'\lambda vU,$$

但是 $UH=H\overline{U}'^{-1}$, 故 $H\overline{U}'^{-1}\overline{v}'\lambda v=H\overline{v}'\lambda vU$, 于是

$$\overline{v}'\lambda v=\overline{(vU)}'\lambda(vU),$$

这表明 vU 与 v 线性相关.

定理 4　设 $U_n(K,H)$ 包有拟对称

$$T=I+H\overline{v}'(vH\overline{v}')^{-1}bv,$$

如 $U_n(K,H)$ 中一个元素 U 与 T 交换, 则 vU 与 v 线性相关, 即 U 将非迷向线 v 保持不变.

【证】　设 $UT=TU$, 则

$$UH\overline{v}'(vH\overline{v}')^{-1}bv=H\overline{v}'(vH\overline{v}')^{-1}bvU.$$

但是 $UH=H\overline{U}'^{-1}$, 故

$$\overline{v}'(vH\overline{v}')^{-1}bv=\overline{(uH)}'(vH\overline{v}')^{-1}b(vU),$$

这表明 vU 与 v 共线.

§10　酉群的中心及射影酉群

设 H 为体 K 上 $n\times n$ 可逆 H- 矩阵. 以 Z 表 K 的中心, Z^* 表 Z 的乘法群. Z^* 中元素 λ 适合 $\lambda\overline{\lambda}=1$ 者显然组成一群. 如 $\lambda\in Z^*$, 而 $\lambda\overline{\lambda}=1$, 则矩阵

$$\lambda I^{(n)}$$

属于 $U_n(K,H)$, 而且易见所有这种元素组成 $U_n(K,H)$ 的一个子群, 记作 $\mathfrak{Z}_n$. 显然, $\mathfrak{Z}_n$ 包含在 $U_n(K,H)$ 的中心之中, 更进一步, 我们证明

定理 1　除开 $K=F_3$, 而 $n=2,\nu=1,\rho=1$ 这一情形, $U_n(K,H)$ 的中心即为 $\mathfrak{Z}_n$.

【证】　先研究 H 的指数 $\nu\geqslant 1$ 的情形. 这时不妨设

$$H=\begin{pmatrix}0 & I^{(\nu)} & 0\\ \rho I^{(\nu)} & 0 & 0\\ 0 & 0 & \varDelta\end{pmatrix}.$$

设 $\varSigma$ 为 $U_n(K,H)$ 的一个中心元素, 先研究 $n>2\nu$ 这一情形. 因 $\varSigma$ 与一切形状

$$\begin{pmatrix}I & -\rho Y\Delta_1\overline{Y}' & Y\\ 0 & I & 0\\ 0 & -\rho\Delta\overline{Y}' & I\end{pmatrix}\quad 及\quad \begin{pmatrix}I & 0 & 0\\ -X\Delta_1\overline{X}' & I & X\\ -\Delta\overline{X}' & 0 & I\end{pmatrix}$$

的酉矩阵皆交换, 其中 X, Y 为任意 $\nu\times(n-2\nu)$ 矩阵, 故 Σ 必为形状

$$\Sigma=\begin{pmatrix} A & 0 & 0 \\ 0 & \overline{A}'^{-1} & 0 \\ 0 & 0 & U \end{pmatrix},$$

而 A, U 适合

(1) $$AY\Delta_1\overline{Y}'=Y\Delta_1\overline{Y}'\overline{A}'^{-1},$$

(2) $$AY=YU,$$

对一切 $\nu\times(n-2\nu)$ 矩阵 Y. 因 Σ 与一切形状

$$\begin{pmatrix} R & 0 & 0 \\ 0 & \overline{R}'^{-1} & 0 \\ 0 & 0 & I \end{pmatrix}\quad (R\in GL_v(K))$$

的矩阵都交换, 故 $A=\lambda I^{(\nu)}$, 而 $\lambda\in Z^*$. 更由 (2) 式推出 $U=\lambda I^{(n-2\nu)}$. 最后, 由 Σ 与

$$\begin{pmatrix} 0 & I^{(\nu)} & 0 \\ \rho I^{(\nu)} & 0 & 0 \\ 0 & 0 & I \end{pmatrix}$$

交换, 推出 $\lambda=\overline{\lambda}^{-1}$, 即 $\lambda\overline{\lambda}=1$. 因此 $\Sigma=\lambda I^{(n)}$, 而 $\lambda\in Z^*$, 适合 $\lambda\overline{\lambda}=1$, 即 $\Sigma\in\mathfrak{Z}_n$.

其次研究 $n=2\nu$ 这一情形. 由 Σ 与

$$\begin{pmatrix} 0 & I^{(\nu)} \\ \rho I^{(\nu)} & 0 \end{pmatrix}$$

交换, 推出 Σ 必为形状

$$\Sigma=\begin{pmatrix} A & B \\ \rho B & A \end{pmatrix}.$$

因 Σ 与一切形状

$$\begin{pmatrix} I^{(\nu)} & P \\ 0 & I^{(\nu)} \end{pmatrix}\quad 及\quad \begin{pmatrix} I^{(\nu)} & 0 \\ Q & I^{(\nu)} \end{pmatrix}$$

的矩阵交换, 其中 P, Q 为任意 $\nu\times\nu$ 矩阵适合 $\overline{P}'=-\rho P, \overline{Q}'=-\rho Q$, 故除了 $\nu=1, K$ 为域, $a\to\overline{a}$ 为单位自同构, $\rho\neq-1$ 这一情形外, Σ 必为形状

$$\Sigma=\begin{pmatrix} A & 0 \\ 0 & A \end{pmatrix}.$$

更由 Σ 与一切形状

$$\begin{pmatrix} R & 0 \\ 0 & \overline{R}'^{-1} \end{pmatrix},$$

其中 $R \in GL_\nu(K)$, 的矩阵交换, 推出 $\Sigma = \lambda I^{(n)}$, 而 $\lambda \in Z^*$, 适合 $\lambda\overline{\lambda} = 1$.

至于当 $\nu = 1, K$ 为域, $a \to \overline{a}$ 为单位自同构, $\rho \neq -1$ 时, $U_2(K, H)$ 即为正交群 $O_2(K, H)$, 而 K 的特征数 $\neq 2$. 如 $K \neq F_3$, 令 $z \in K^*$, 而 $z \neq \pm 1$, 则由 Σ 与

$$\begin{pmatrix} z & 0 \\ 0 & z^{-1} \end{pmatrix}$$

交换, 推出 $\Sigma = \lambda I^{(2)}$, 而 $\lambda \in K^* = Z^*$ 适合 $\lambda\overline{\lambda} = \lambda^2 = 1$.

至于 $O_2\left(F_3, \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}\right)$ 这一情形, 确为一例外情形. 易见

$$O_2\left(F_3, \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}\right)$$

由下列四个元素组成:

$$\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} -1 & 0 \\ 0 & -1 \end{pmatrix}, \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}, \begin{pmatrix} 0 & -1 \\ -1 & 0 \end{pmatrix}.$$

显然, $O_2\left(F_3, \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}\right)$ 是交换群, 因而与它的中心相重.

最后我们研究 H 的指数 $\nu = 0$ 的情形. 仍设 Σ 为 $U_n(K, H)$ 的一个中心元素. 因 Σ 与 $U_n(K, H)$ 中每一个拟对称交换, 而对于任一 n 维非迷向向量 $v, U_n(K, H)$ 至少存在着一个拟对称

$$I - 2H\overline{v}'(vH\overline{v}')^{-1}v,$$

即对称. 因此 Σ 将每个 n 维非迷向向量都保持不变. 因 H 的指数 $\nu = 0$. 这时每个 n 维向量都是非迷向的, 所以 Σ 将每个 n 维向量都保持不变. 从 Σ 将下面这 n 个 n 维向量:

$$(1, 0, \cdots, 0), \quad (0, 1, 0, \cdots, 0), \cdots, (0, \cdots, 0, 1)$$

保持不变, 推出 Σ 为对角形矩阵. 从 Σ 将 n 维向量

$$(1, 1, \cdots, 1)$$

保持不变, 推出 $\Sigma = \lambda I^{(n)}$. 再从 Σ 将一切形为

$$(x, 1, \cdots, 1) \quad (x \in K^*)$$

的 n 维向量保持不变, 推出 $\lambda \in Z^*$. 因 $\Sigma \in U_n(K,H)$, 故 $\lambda\bar{\lambda}=1$. 这就证明了 $\Sigma \in \mathfrak{Z}_n$. 定理至此证毕.

我们回忆, $GL_n(K)$ 的中心是 Z_n. 因此除了 $K=F_3, n=2, \nu=1$ 这一情形, 即 $O_2\left(F_3, \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}\right)$ 这一情形之外, 我们有

$$\mathfrak{Z}_n = U_n(K,H) \cap Z_n.$$

作为定理 1 的特例, 我们有

系理 1 域 K 上的辛群 $Sp_{2\nu}(K)$ 的中心仅由 $\pm I$ 两个元素组成.

系理 2 特征数 $\neq 2$ 的域 K 上的指数 $\geqslant 1$ 的正交群 $O_n(K,H)$ 的中心仅由 $\pm I$ 两个元素组成, 除开 $O_2\left(F_3, \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}\right)$ 这个例外情形.

以前我们把 $GL_n(K)$ 对其中心 Z_n 的商群称为射影一般线性群, 记作 $PGL_n(K)$. 现在我们把 $U_n(K,H)$ 在自然同态

$$GL_n(K) \to PGL_n(K)$$

之下的像称为射影酉群, 记作 $PU_n(K,H)$. 因此, 除了 $O_2\left(F_3, \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}\right)$ 之外, 我们有

$$PU_n(K,H) \cong U_n(K,H)/\mathfrak{Z}_n.$$

同样我们可以定义 $PO_n^+(K,H)$ 及 $PU_n^+(K,H)$.

§11 有限域上的酉群

定理 1 设 p 为素数而 $q=p^n$. 以 F_q 表 q 个元素的有限域. 于是辛群 $Sp_{2\nu}(F_q)$ 的阶为

$$(q^{2\nu}-1)q^{2\nu-1}(q^{2\nu-2}-1)q^{2\nu-3}\cdots(q^2-1)q.$$

【证】 设

$$T = \begin{pmatrix} a_{11} & \cdots & a_{1\nu} & b_{11} & \cdots & b_{1\nu} \\ & \cdots & & & \cdots & \\ a_{\nu 1} & \cdots & a_{\nu\nu} & b_{\nu 1} & \cdots & b_{\nu\nu} \\ c_{11} & \cdots & c_{1\nu} & d_{11} & \cdots & d_{1\nu} \\ & \cdots & & & \cdots & \\ c_{\nu 1} & \cdots & c_{\nu\nu} & d_{\nu 1} & \cdots & d_{\nu\nu} \end{pmatrix}$$

为 $Sp_{2\nu}(F_q)$ 中任一元素. 首先, 我们断言, 存在一个辛矩阵 P, 使得 PT 的 $(1,1)$ 位置元素 $\neq 0$. 实际上, 如 $a_{11}\neq 0$, 取 $P=I$ 即可. 如 $a_{11}=0$ 而 $a_{21},\cdots,a_{\nu 1}$ 中至少有一个不为 0, 设足码最小的不为 0 者是 a_{i1}. 取

$$P=\begin{pmatrix} A & 0 \\ 0 & A'^{-1} \end{pmatrix},$$

而

$$A=E_{1i}+E_{i1}+\sum_{\substack{j=2\\ j\neq i}}^{\nu}E_{jj}.$$

如果 $a_{11}=a_{21}=\cdots=a_{\nu 1}=0$, 那么 $c_{11},\cdots,c_{\nu 1}$ 中至少有一不为 0, 设足码最小的不为 0 者是 c_{i1}. 取

$$P=\begin{pmatrix} [0,1,\cdots,1] & [1,0,\cdots,0] \\ [-1,0,\cdots,0] & [0,1,\cdots,1] \end{pmatrix}\begin{pmatrix} A & 0 \\ 0 & A'^{-1} \end{pmatrix},$$

其中

$$\begin{aligned} &A=I, && \text{如} i=1,\\ &A=E_{1i}+E_{i1}+\sum_{\substack{j=2\\ j\neq i}}^{\nu}E_{ii}, && \text{如} i\neq 1. \end{aligned}$$

这就证明了我们的断言. 我们注意, 根据我们规定的取法, P 由 T 唯一确定. 令 $PT=T_1$.

现在假定 $a_{11}\neq 0$. 令

$$T_2=\begin{pmatrix} I & 0 \\ S & I \end{pmatrix}\begin{pmatrix} V & 0 \\ 0 & V'^{-1} \end{pmatrix}\begin{pmatrix} [a_{11}^{-1},1,\cdots,1] & 0 \\ 0 & [a_{11},1,\cdots,1] \end{pmatrix}T_1,$$

其中

$$S=\begin{pmatrix} -\sum_{i=1}^{\nu}a_{i1}c_{i1} & -c_{21} & \cdots & -c_{\nu 1} \\ -c_{21} & & & \\ \vdots & & 0 & \\ -c_{\nu 1} & & & \end{pmatrix},$$

$$V=\begin{pmatrix} 1 & 0 & \cdots & 0 \\ -a_{21} & 1 & & \\ \vdots & & \ddots & 0 \\ -a_{\nu 1} & 0 & & 1 \end{pmatrix},$$

于是, T_2 有以下形状:

$$T_2 = \begin{pmatrix} 1 & a_{12} & \cdots & a_{1\nu} & b_{11} & \cdots & b_{1\nu} \\ 0 & a_{22} & \cdots & a_{2\nu} & b_{21} & \cdots & b_{2\nu} \\ \vdots & & \cdots & & & \cdots & \\ 0 & a_{\nu 2} & \cdots & a_{\nu\nu} & b_{\nu 1} & \cdots & b_{\nu\nu} \\ 0 & c_{12} & \cdots & c_{1\nu} & d_{11} & \cdots & d_{1\nu} \\ \vdots & & \cdots & & & \cdots & \\ 0 & c_{\nu 2} & \cdots & c_{\nu\nu} & d_{\nu 1} & \cdots & d_{\nu\nu} \end{pmatrix}.$$

因为 T_2 是辛矩阵, $A'D - C'B = I$. 因此 $d_{11} = 1$. 令

$$T_3 = \begin{pmatrix} I & S_1 \\ 0 & I \end{pmatrix} \begin{pmatrix} V_1 & 0 \\ 0 & V_1'^{-1} \end{pmatrix} T_2,$$

其中

$$S_1 = \begin{pmatrix} -\sum_{i=1}^{\nu} d_{i1} db_{i1} & -b_{21} & \cdots & -b_{\nu 1} \\ -b_{21} & & & \\ \vdots & & & 0 \\ -b_{\nu 1} & & & \end{pmatrix},$$

$$V_1 = \begin{pmatrix} 1 & d_{21} & \cdots & d_{\nu 1} \\ 0 & 1 & & 0 \\ \vdots & & \ddots & \\ 0 & 0 & & 1 \end{pmatrix},$$

则 T_3 有形状

$$T_3 = \begin{pmatrix} 1 & a_{12} & \cdots & a_{1\nu} & 0 & b_{12} & \cdots & b_{1\nu} \\ 0 & a_{22} & \cdots & a_{2\nu} & 0 & b_{22} & \cdots & b_{2\nu} \\ \vdots & & \cdots & & \vdots & & \cdots & \\ 0 & a_{\nu 2} & \cdots & a_{\nu\nu} & 0 & b_{\nu 2} & \cdots & b_{\nu\nu} \\ 0 & c_{12} & \cdots & c_{1\nu} & 1 & d_{12} & \cdots & d_{1\nu} \\ 0 & c_{22} & \cdots & c_{2\nu} & 0 & d_{22} & \cdots & d_{2\nu} \\ \vdots & & \cdots & & \vdots & & \cdots & \\ 0 & c_{\nu 2} & \cdots & c_{\nu\nu} & 0 & d_{\nu 2} & \cdots & d_{\nu\nu} \end{pmatrix}.$$

又因 T_3 是辛矩阵, 故有

$$a_{1i} = b_{1i} = c_{1i} = d_{1i} = 0 \quad (i = 2, 3, \cdots, \nu).$$

即

$$T_3 = \begin{pmatrix} 1 & 0 & \cdots & 0 & 0 & 0 & \cdots & 0 \\ 0 & a_{22} & \cdots & a_{2\nu} & 0 & b_{22} & \cdots & b_{2\nu} \\ \vdots & & \cdots & & \vdots & & \cdots & \\ 0 & a_{\nu 2} & \cdots & a_{\nu\nu} & 0 & b_{\nu 2} & \cdots & b_{\nu\nu} \\ 0 & 0 & \cdots & 0 & 1 & 0 & \cdots & 0 \\ 0 & c_{22} & \cdots & c_{2\nu} & 0 & d_{22} & \cdots & d_{2\nu} \\ \vdots & & \cdots & & \vdots & & & \\ 0 & c_{\nu 2} & \cdots & c_{\nu\nu} & 0 & d_{\nu 2} & \cdots & d_{\nu\nu} \end{pmatrix}.$$

因此 T_3 是 $\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$ 和 $2(\nu-1)$ 阶辛阵

$$\begin{pmatrix} a_{22} & \cdots & a_{2\nu} & b_{22} & \cdots & b_{2\nu} \\ & \cdots & & & \cdots & \\ a_{\nu 2} & \cdots & a_{\nu\nu} & b_{\nu 2} & \cdots & b_{\nu\nu} \\ c_{22} & \cdots & c_{2\nu} & d_{22} & \cdots & d_{2\nu} \\ & \cdots & & & \cdots & \\ c_{\nu 2} & \cdots & c_{\nu\nu} & d_{\nu 2} & \cdots & d_{\nu\nu} \end{pmatrix}$$

的直和.

注意, 在 T 中, $a_{11}, \cdots, a_{\nu 1}, c_{11} \cdots, c_{\nu 1}$ 一共可取 $q^{2\nu}-1$ 组不全为 0 的值; 当 T 确定之后, T_1 就唯一确定, 于是 T_2 也就被唯一确定. 在 T_2中, $b_{11}, \cdots, b_{v1}, d_{21}, \cdots, d_{v1}$ 一共可取 $q^{2\nu-1}$ 组值, 当 T_2 确定后, T_3 就唯一确定. 因此有递推公式

$$Sp_{2\nu}(F_q) : 1 = (q^{2\nu}-1)q^{2\nu-1}[Sp_{2(\nu-1)}(F_q) : 1].$$

因

$$Sp_2(F_q) : 1 = SL_2(F_q) : 1 = (q^2-1)q,$$

所以

$$Sp_{2\nu}(F_q) : 1 = (q^{2\nu}-1)q^{2(\nu-1)}(q^{2(\nu-1)}-1)q^{2\nu-3}\cdots(q^2-1)q.$$

这样定理 1 就证明了.

利用类似的方法, 可以证明

定理 2 $U_n(F_{q^2})$ 的阶是

$$(q^n-(-1)^n)q^{n-1}(q^{n-1}-(-1)^{n-1})q^{n-2}\cdots(q^2-1)q(q+1).$$

定理 3 当 n 是奇数时 (这时 F_q 上 n 级正交群皆同构), $O_n^+(F_q)$ 的阶为

$$(q^{n-1}-1)q^{n-2}(q^{n-3}-1)q^{n-4}\cdots(q^2-1)q;$$

而当 $n=2m$ 是偶数时, $O_n^+(F_q,H)$ 的阶是

$$(q^{2m-1}-\varepsilon q^{m-1})(q^{2m-2}-1)q^{2m-3}\cdots(q^2-1)q,$$

其中 $\varepsilon=1$ 如果 $(-1)^m\det H$ 是 F_q 中平方元素, 而 $\varepsilon=-1$, 如果 $(-1)^m\det H$ 不是 F_q 中平方元素.

第八章　酉群的构造 ($\nu \geqslant 1$ 而正交群除外)

§1　引　　言

我们假定 K 为体, $a \to \bar{a}$ 为 K 之对合. 设 H 为 K 上 $n \times n$ 可逆 H- 矩阵, 其标元 $\rho = -1$. (注意, $\rho = -1$ 的假设只排除了特征数 $\neq 2$ 的域上的对称矩阵, 因为当 $a \to \bar{a}$ 不是单位自同构时, K 上哈矩阵的研究皆可化归我们所讨论的情形.) 因此不妨设

$$H = \begin{pmatrix} 0 & I^{(\nu)} & 0 \\ -I^{(\nu)} & 0 & 0 \\ 0 & 0 & \Delta \end{pmatrix},$$

其中 $\overline{\Delta}' = -\Delta$ 为 $n - 2\nu$ 行的对角形定号 H- 矩阵, 于是 ν 为 H 的指数. 当 H 是斜对称矩阵时, $\Delta = 0$; 当 $\Delta \neq 0$ 时, 恒有 $n - 2\nu$ 行可逆对角形矩阵 Δ_1, 使 $\Delta = \Delta_1 - \overline{\Delta}_1$.

前一章里, 我们已经定义了, $U_n(K, H)$ 中的一个矩阵 T 称为酉平延, 如 $T - I$ 是秩为 1 的幂零矩阵. $U_n(K, H)$ 中所有的平延生成 $U_n(K, H)$ 的一个子群, 称为酉平延群, 记作 $TU_n(K, H)$. 因酉平延在酉矩阵之下的变形仍为酉平延, 故 $TU_n(K, H)$ 为 $U_n(K, H)$ 的正规子群. 以 W_n 表 $TU_n(K, H)$ 的中心, 我们有 $U_n(K, H)$ 的正规群列:

$$U_n(K, H) \supset TU_n(K, H) \supset W_n \supset \{I\}.$$

本章目的就是研究这个正规群列的三个因子:

$$U_n(K, H)/TU_n(K, H), \quad TU_n(K, H)/W_n, \quad W_n$$

的构造. 特别, 我们还把 $TU_n(K, H)/W_n$ 记作 $PTU_n(K, H)$, 称为射影酉平延群.

为了以后的需要, 我们先证明次之引理.

引理 1　设 K 不是域, 则 K 中对称元素的全体 S 所生成之子体 $K_1 = K$, 除非 K 是特征数 $\neq 2$ 的域 Z 上的广义四元数体, 而这时 $S = Z$.

【证】　我们先证明 S 生成之子环即为 K_1. 实际上, 设 ζ 是这个子环中的任一非零元素, 则 $\bar{\zeta}$ 亦属于这个子环. 但是 $\zeta\bar{\zeta} = \delta \in S$, 所以 $\zeta^{-1} = \bar{\zeta}\delta^{-1}$ 就属于 S 生成之子环. 因此 S 生成之子环即为 K_1.

其次我们断言

(1)　$$kk_1 - k_1k \in K_1, \text{对一切} k \in K, k_1 \in K_1.$$

实际上, 只要证明 (1) 对于一切 $k_1 = s_1s_2\cdots s_m(s_1 \in S)$ 成立即可. 我们用归纳法向 m 来证明这件事实. 先设 $m=1$, 即 $k_1 = s_1$, 这时由 $ks_1+\overline{ks_1} \in S$ 及 $s_1(k+\bar{k}) \in K_1$ 推出

$$ks_1 - s_1k = ks_1 + s_1\bar{k} - s_1(k+\bar{k}) \in K_1.$$

次设 $m>1$, 并假定断言对 $m-1$ 成立. 令 $s' = s_1\cdots s_{m-1}$, 则 $s = s's_m$. 于是由 $ks' = s'k \in K_1$ 及 $s_mk - ks_m \in K_1$ 推出

$$ks - sk = ks's_m - s's_mk = (ks' - s'k)s_m - s'(s_mk - ks_m),$$

所以我们的断言对 m 也成立.

设 K_1 不是域, 则存在 $k_1, k_2 \in K_1$, 使 $k_1k_2 \neq k_2k_1$. 今在 (1) 中取 k 为 kk_2, 则

$$kk_2k_1 - k_1kk_2 = k(k_2k_1 - k_1k_2) + (kk_1 - k_1k)k_2 \in K_1.$$

由于 $k_2k_1 - k_1k_2, kk_1 - k_1k, k_2 \in K_1$ 而 $k_2k_1 - k_1k_2 \neq 0$, 故 $k \in K_1$. 这表明 $K_1 = K$.

现在设 K_1 是域. 因此 S 中任意二元素皆可换, 故 K_1 中元素皆是对称元素, 所以 $K_1 = S$. 任取 $k(\neq 0) \in K$ 及 $s \in S$. 因 $k\bar{k} \in S$, 故 $k\bar{k}s = sk\bar{k}$, 将此式改写为

$$k^{-1}sk = \bar{k}s\bar{k}^{-1} = \overline{k^{-1}sk},$$

所以 $k^{-1}sk \in K_1 = S$, 即 K_1 是 K 的正规子体. 由第一章定理 11.2, 推出 $K_1 \subset Z$.

因 K 不是域, 故有 $k \in K$ 而 $k \notin Z$. 设 z 为 Z 中任意元素, 则 $zk + \overline{zk} \in S \subset Z$. 可是

$$zk + \overline{zk} = zk + \bar{k}\bar{z} = z(k+\bar{k}) + \bar{k}(\bar{z} - z),$$

其中 $z(k+\bar{k}) \in Z, \bar{z} - z \in Z$. 由于 $\bar{k} \notin Z$, 故只有 $\bar{z} - z = 0$ 才可能. 所以 $\bar{z} = z$ 对一切 $z \in Z$. 这就证明了 $S = Z$.

设 $x \in K, x \notin Z$. 则 $x + \bar{x} \in Z, \bar{x}x \in Z$. 于是

$$x^2 - (x+\bar{x})x + \bar{x}x = 0,$$

即 K 中任一不属于 Z 之元素皆满足 Z 上一个二次方程. 依第一章定理 10.1, K 是 Z 上广义四元数体. 如果 K_1 的特征数 $=2$, $S \neq Z$. 所以 K 的特征数 $\neq 2$.

这样, 引理 1 就完全证明了.

我们还需要下面的

引理 2 设 A 是 $n \times n$ 可逆哈矩阵, 则 $\det A \in S^*C/C$, 其中 S^* 表 S 中非 0 元素生成之群, S^*C 表由 S^* 和 C 所生成之群.

【证】 如 A 为交错矩阵 (这时 K 是特征数 $=2$ 的域), 引理 2 自然成立. 设 A 不是交错的, 于是有 $n \times n$ 可逆矩阵 P, 使

$$A = P\begin{pmatrix} \lambda_1 & & & \\ & \lambda_2 & & 0 \\ 0 & & \ddots & \\ & & & \lambda_n \end{pmatrix}\bar{P}' \quad (\bar{\lambda}_i = \lambda_i; i = 1, 2, \cdots, n).$$

因之

$$\det A = \det P \ \det \bar{P}' \lambda_1 \lambda_2 \cdots \lambda_n C,$$

所以我们只要证明 $\det P \ \det \bar{P}' \in S^* C/C$ 即可. 写 $P = BD(\mu)$, 其中 $B \in SL_n(K)$, $D(\mu) = [1, 1, \cdots, 1, \mu]$ $(\mu \neq 0)$. 则 $\bar{P}' = D(\bar{\mu})\bar{B}'$. 因之

$$\det P \ \det \bar{P}' = \mu C \bar{\mu} C = \mu \bar{\mu} C \in S^* C/C.$$

因此引理 2 证毕.

§2 $TU_n(K, H)$ 的中心

为了研究 $TU_n(K, H)$ 的中心, 我们先列举出 $TU_n(K, H)$ 的一批元素来, 这就是

定理 1 设 $v \geqslant 1$, 以下这些元素都属于 $TU_n(K, H)$:

(1)
$$\begin{pmatrix} I^{(\nu)} & Y & \\ & I^{(\nu)} & \\ & & I^{(n-2\nu)} \end{pmatrix} \quad (\bar{Y}' = Y);$$

(2)
$$\begin{pmatrix} I^{(\nu)} & & \\ X & I^{(\nu)} & \\ & & I^{(n-2\nu)} \end{pmatrix} \quad (\bar{X}' = X);$$

(3)
$$\begin{pmatrix} I - J & J & \\ -J & I - J & \\ & & J \end{pmatrix} \quad (J^2 = J\text{为对角形矩形});$$

(4)
$$\begin{pmatrix} A & & \\ & \bar{A}'^{-1} & \\ & & I \end{pmatrix} \quad (A \in SL_\nu(K), \text{若}\nu \geqslant 2);$$

(5)
$$\begin{pmatrix} \lambda I & & \\ & \bar{\lambda}^{-1}I & \\ & & I \end{pmatrix} \quad (\bar{\lambda}=\lambda\neq 0);$$

(6)
$$\begin{pmatrix} I & P\varDelta_1\bar{P}' & P \\ & I & \\ & \varDelta\bar{P}' & I \end{pmatrix} \quad (P=P^{(\nu,n-2\nu)}),$$

若 $TU_n(K,H)\neq TU_3\left(F_4,\begin{pmatrix} 0&1&0\\ 1&0&0\\ 0&0&1 \end{pmatrix}\right)$, 而 $a\to\bar{a}$ 不是单位自同构;

(7)
$$\begin{pmatrix} I & & \\ -Q\varDelta_1\bar{Q}' & I & Q \\ -\varDelta\bar{Q}' & & I \end{pmatrix} \quad (Q=Q^{(\nu,n-2\nu)}),$$

若 $TU_n(K,H)\neq TU_3\left(F_4,\begin{pmatrix} 0&1&0\\ 1&0&0\\ 0&0&1 \end{pmatrix}\right)$, 而 $a\to\bar{a}$ 不是单位自同构.

【证】 在证明 (1) ~ (5) 属于 $TU_n(K,H)$ 时, 无妨设 $n=2\nu$.

首先, 设 $\bar{Y}'=Y$ 而 Y 不是交错矩阵. 于是有 $\nu\times\nu$ 可逆矩阵 P, 使

$$PY\bar{P}'=[\lambda_1,\cdots,\lambda_r,0,\cdots,0] \quad (\overline{\lambda_i}=\lambda_i;i=1,\cdots,r).$$

于是

$$\begin{aligned}\begin{pmatrix} I & Y \\ & I \end{pmatrix}&=\begin{pmatrix} P^{-1} & \\ & \bar{P}' \end{pmatrix}\begin{pmatrix} I & [\lambda_1,\cdots,\lambda_r,0,\cdots,0] \\ & I \end{pmatrix}\begin{pmatrix} P^{-1} & \\ & \bar{P}' \end{pmatrix}^{-1}\\ &=\begin{pmatrix} P^{-1} & \\ & \bar{P}' \end{pmatrix}\begin{pmatrix} I & [\lambda_1,0,\cdots,0] \\ & I \end{pmatrix}\begin{pmatrix} P^{-1} & \\ & \bar{P}' \end{pmatrix}^{-1}\cdots\\ &\quad\cdot\begin{pmatrix} P^{-1} & \\ & \bar{P}' \end{pmatrix}\begin{pmatrix} I & [0,\cdots,0,\lambda_r,0,\cdots,0] \\ & I \end{pmatrix}\begin{pmatrix} P^{-1} & \\ & \bar{P}' \end{pmatrix}^{-1}\end{aligned}$$

是一些酉平延之积, 因而属于 $TU_n(K,H)$. 若 Y 是交错矩阵, 这时 K 是特征数 $=2$ 的域而 $a\to\bar{a}$ 是单位自同构, 于是 $Y+[1,0,\cdots,0]$ 不是交错矩阵. 因之

$$\begin{pmatrix} I & Y \\ & I \end{pmatrix}=\begin{pmatrix} I & [1,0,\cdots,0] \\ & I \end{pmatrix}\begin{pmatrix} I & Y+[1,0,\cdots,0] \\ & I \end{pmatrix}\in TU_n(K,H).$$

同理可证 (2) 也属于 $TU_n(K,H)$.

注意到

$$\begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix} = \begin{pmatrix} 1 & 1 \\ & 1 \end{pmatrix} \begin{pmatrix} 1 & \\ -1 & 1 \end{pmatrix} \begin{pmatrix} 1 & 1 \\ & 1 \end{pmatrix},$$

由此及 (1), (2) 属于 $TU_n(K,H)$ 即可推出 (3) 也属于 $TU_n(K,H)$.

我们来证 (4) 属于 $TU_n(K,H)$. 为书写方便起见, 设 $n = 2\nu = 4$. 我们有

$$\begin{pmatrix} I & \begin{pmatrix} 0 & \lambda \\ \bar{\lambda} & 0 \end{pmatrix} \\ & I \end{pmatrix} \begin{pmatrix} I & \\ \begin{pmatrix} 0 & 0 \\ 0 & 1 \end{pmatrix} & I \end{pmatrix} = \begin{pmatrix} \begin{pmatrix} 1 & \lambda \\ 0 & 1 \end{pmatrix} & \begin{pmatrix} 0 & \lambda \\ \bar{\lambda} & 0 \end{pmatrix} \\ \begin{pmatrix} 0 & 0 \\ 0 & 1 \end{pmatrix} & I \end{pmatrix}$$

属于 $TU_n(K,H)$. 利用 (1), (2) 属于 $TU_n(K,H)$ 即可推出

$$\begin{pmatrix} 1 & \lambda & & \\ 0 & 1 & & \\ & & 1 & 0 \\ & & -\bar{\lambda} & 1 \end{pmatrix} \in TU_4(K,H).$$

同理可证

$$\begin{pmatrix} 1 & 0 & & \\ \mu & 1 & & \\ & & 1 & -\bar{\mu} \\ & & 0 & 1 \end{pmatrix} \in TU_4(K,H).$$

因 $SL_2(K)$ 由一切 $B_{12}(\lambda)$ 和 $B_{12}(\mu)$ 生成, 故 (4) 也属于 $TU_n(K,H)$.

再证 (5) 属于 $TU_n(K,H)$. 为书写方便起见, 设 $n = 2, \nu = 1$. 对任意 $\bar{\mu} = \mu$, 我们有

$$\begin{pmatrix} 1 & 1 \\ & 1 \end{pmatrix} \begin{pmatrix} 1 & \\ \mu & 1 \end{pmatrix} = \begin{pmatrix} 1+\mu & 1 \\ \mu & 1 \end{pmatrix} \in TU_2(K,H).$$

再利用 (1), (2) 属于 $TU_n(K,H)$ 即推出

$$\begin{pmatrix} 1+\mu & \\ & (1+\mu)^{-1} \end{pmatrix} \in TU_2(K,H).$$

对一切 $\bar{\mu} = \mu \neq -1$. 因此 (5) 也属于 $TU_n(K,H)$.

最后来证明 (6) 也属于 $TU_n(K,H)$, 若

$$TU_n(K,H) \neq TU_3\left(F_4, \begin{pmatrix} 0 & 1 & \\ 1 & 0 & \\ & & 1 \end{pmatrix}\right),$$

而 $a\to\bar{a}$ 不是单位自同构. 注意

$$\begin{pmatrix} I & P\varDelta_1\bar{P}' & P \\ & I & \\ & \varDelta\bar{P}' & I \end{pmatrix}\begin{pmatrix} I & Q\varDelta_1\bar{Q}' & Q \\ & I & \\ & \varDelta\bar{Q}' & I \end{pmatrix}$$

$$=\begin{pmatrix} I & P\varDelta_1\bar{P}'+Q\varDelta_1\bar{Q}'+P\varDelta\bar{Q}' & P+Q \\ & I & \\ & \varDelta\overline{(P+Q)}' & I \end{pmatrix}$$

$$=\begin{pmatrix} I & Y & \\ & I & \\ & & I \end{pmatrix}\begin{pmatrix} I & (P+Q)\varDelta_1\overline{(P+Q)}' & P+Q \\ & I & \\ & \varDelta\overline{(P+Q)}' & I \end{pmatrix},$$

其中 $Y=-Q\varDelta_1\bar{P}'-P\overline{\varDelta}_1'\bar{Q}'$ 为哈矩阵. 因此只要证 (6) 属于 $TU_n(K,H)$ 对仅一行不为 0 的 P 即可. 我们研究

$$\varSigma=\begin{pmatrix} A & & \\ & \bar{A}'^{-1} & \\ & & I \end{pmatrix}\begin{pmatrix} I & P\varDelta_1\bar{P}' & P \\ & I & \\ & \varDelta\bar{P}' & I \end{pmatrix}\begin{pmatrix} A & & \\ & \bar{A}'^{-1} & \\ & & I \end{pmatrix}^{-1}\begin{pmatrix} I & P\varDelta_1\bar{P}' & P \\ & I & \\ & \varDelta\bar{P}' & I \end{pmatrix}^{-1}$$

$$=\begin{pmatrix} I & AP\varDelta_1\bar{P}'\bar{A}'-AP\varDelta\bar{P}'-P\bar{\varDelta}_1\bar{P}' & (A-I)P \\ & I & \\ & \varDelta\overline{(A-I)P}' & I \end{pmatrix}$$

$$=\begin{pmatrix} I & Y & \\ & I & \\ & & I \end{pmatrix}\begin{pmatrix} I & (A-I)P\varDelta_1\overline{(A-I)P}' & (A-I)P \\ & I & \\ & \varDelta\overline{(A-I)P}' & I \end{pmatrix},$$

其中 $Y=AP\overline{\varDelta}_1'\bar{Q}'\bar{P}'+P\varDelta_1\bar{P}'\bar{A}'-P(\varDelta_1+\overline{\varDelta}_1'\bar{Q}')\bar{P}'$ 为哈矩阵. 若 $\nu\geqslant 2$, 可选取 $A\in SL_\nu(K)$ 及 P, 使 $(A-I)P$ 跑过仅一行不为 0 的 P, 于是从 $\varSigma\in TU_n(K,H)$ 推出 (6) 属于 $TU_n(K,H)$ 对仅一行不为 0 的 P. 若 $\nu=1$, 可选取 $A=\lambda=\bar{\lambda}\neq 0,1$, 同样可推出 (6) 属于 $TU_n(K,H)$. 若 $\nu=1$, 而 $S=\{0,1\}$, 则依引理 1.1, K 为域, 因之 $K=F_4$; 这时一定有 $n=3$, 这正是我们除外的情形.

同理可证 (7) 也属于 $TU_n(K,H)$.

定理 1 至此完全证毕.

系理 如 $U_n(K,H)=Sp_n(K)$, 则 $TU_n(K,H)=Sp_n(K)$.

定理 2 设 $\nu\geqslant 1$, 则 $TU_n(K,H)$ 的中心 $W_n=Z_n\cap TU_n(K,H)$, Z_n 表 $GL_n(K)$ 的中心, 即 W_n 仅含中心矩阵.

【证】 设

$$\Sigma = \begin{pmatrix} A & B & P \\ C & D & Q \\ R & T & U \end{pmatrix}$$

是 W_n 的一个元素. 因 $\sum$ 与一切形状

$$\begin{pmatrix} I & & \\ X & I & \\ & & I \end{pmatrix} \text{ 及 } \begin{pmatrix} I & Y & \\ & I & \\ & & I \end{pmatrix} \quad (\bar{X}' = X, \bar{Y}' = Y)$$

的元素都交换, 故 $B = C = 0, P = Q = 0, R = T = 0$, 而且

$$XA = DX, \text{对一切} \bar{X}' = X.$$

在上式中令 $X = I$, 得 $A = D$. 再由 $XA = AX$ 对一切 $\bar{X}' = X$ 推出 $A = \lambda I$. 因之

$$\Sigma = \begin{pmatrix} \lambda I & & \\ & \lambda I & \\ & & U \end{pmatrix}.$$

又因 $\Sigma \in TU_n(K, H)$, 故 $\lambda\bar{\lambda} = 1$. 分以下两个情形来讨论:

(i) $\nu \geqslant 2$. 因 Σ 与一切元素

$$\begin{pmatrix} A & & \\ & \bar{A}'^{-1} & \\ & & I \end{pmatrix} \quad (A \in SL_\nu(K))$$

都交换, 故 $\lambda \in Z^*$. 因此, 当 $n = 2\nu$ 时, 定理 2 已经证明. 现在设 $n - 2\nu > 0$, 由 Σ 与一切形状

$$\begin{pmatrix} I & P\Delta_1\bar{P}' & P \\ & I & \\ & \Delta\bar{P}' & I \end{pmatrix} \quad (P = P^{(\nu, n-2\nu)})$$

的元素都交换, 故 $\lambda P = PU$ 对一切 $\nu \times (n - 2\nu)$ 矩阵 P. 因此 $U = \lambda I$. 故这时本定理也成立.

(ii) $\nu = 1$. 先考查 $n \geqslant 3$ 的情形. 如 $TU_n(K, H) \neq TU_3(F_4, H)$, 则由 Σ 与一切形状

$$\begin{pmatrix} 1 & p\Delta_1\bar{p}' & p \\ & 1 & \\ & \Delta\bar{p}' & I \end{pmatrix} \quad (p = p^{(1, n-2)})$$

的元素都交换, 推出 $\lambda p = pU$ 对一切 $1\times(n-2)$ 矩阵 p, 故 $U=\lambda I$ 而 $\lambda\in Z^*$. 这时本定理也成立.

设 $TU_n(K,H)=TU_3\left(F_4,\begin{pmatrix}0&1&\\1&0&\\&&1\end{pmatrix}\right)$. 令 $F_4=F_2(x)$, 而 $x^2+x+1=0$, 则 $\bar{x}=x+1$. 于是 $(x,1,1)$ 是对于 $\begin{pmatrix}0&1&\\1&0&\\&&1\end{pmatrix}$ 的迷向向量. 那么以 $(x,1,1)$ 为迷向向量的酉平延是

$$\begin{aligned}T&=I+H\overline{(x,1,1)}'(x,1,1)\\&=I+\begin{pmatrix}0&1&\\1&0&\\&&1\end{pmatrix}\begin{pmatrix}\bar{x}x&\bar{x}&\bar{x}\\x&1&1\\x&1&1\end{pmatrix}\\&=I+\begin{pmatrix}x&1&1\\\bar{x}x&\bar{x}&\bar{x}\\x&1&1\end{pmatrix}=\begin{pmatrix}\bar{x}&1&1\\1&x&\bar{x}\\x&1&0\end{pmatrix}\end{aligned}$$

(注意 $\bar{x}=1+x, x\bar{x}=1$). 那么由

$$\begin{pmatrix}\lambda&&\\&\lambda&\\&&u\end{pmatrix}\begin{pmatrix}\bar{x}&1&1\\1&x&\bar{x}\\x&1&0\end{pmatrix}=\begin{pmatrix}\bar{x}&1&1\\1&x&\bar{x}\\x&1&0\end{pmatrix}\begin{pmatrix}\lambda&&\\&\lambda&\\&&u\end{pmatrix}$$

推出 $\lambda=u$. 所以这时定理也成立.

最后我们研究 $n=2$ 的情形. 如 K 是域, 本定理自然成立. 今设 K 不是域. 这时由

$$\begin{pmatrix}\lambda&\\&\lambda\end{pmatrix}\begin{pmatrix}a&\\&\bar{a}^{-1}\end{pmatrix}=\begin{pmatrix}a&\\&\bar{a}^{-1}\end{pmatrix}\begin{pmatrix}\lambda&\\&\lambda\end{pmatrix}$$

对一切 $\bar{a}=a\in K^*$, 推出 $\lambda a=a\lambda$ 对一切 $\bar{a}=a\in K^*$. 因此根据引理 1.1, 如 K 不是特征数 $\neq 2$ 的广义四元数体, 则 $\lambda\in Z^*$. 如果 K 是特征数 $\neq 2$ 的广义四元数体, 这时本定理仍然成立, 但这是下面定理的系理的推论.

定理 3 $TU_2\left(K,\begin{pmatrix}0&1\\-1&0\end{pmatrix}\right)$ 由一切

$$\begin{pmatrix}1&\lambda\\0&1\end{pmatrix}\quad 及\quad \begin{pmatrix}1&0\\\mu&1\end{pmatrix}\quad(\bar{\lambda}=\lambda,\bar{\mu}=\mu)$$

所生成.

【证】 设 (a,b) 是一个迷向向量, 即

$$(a,b)\begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}\begin{pmatrix} \bar{a} \\ \bar{b} \end{pmatrix} = 0,$$

$$a\bar{b} - b\bar{a} = 0.$$

如 $b \neq 0, b^{-1}a$ 为对称元素. 以 (a,b) 为迷向向量的酉平延是

$$\begin{aligned} T &= I + H\overline{(a,b)}'\lambda(a,b) \\ &= \begin{pmatrix} 1+\bar{b}\lambda a & \bar{b}\lambda b \\ -\bar{a}\lambda a & 1-\bar{a}\lambda b \end{pmatrix} \quad (\bar{\lambda} = \lambda \neq 0). \end{aligned}$$

如果 $b = 0$, 则

$$T = \begin{pmatrix} 1 & 0 \\ -\bar{a}\lambda a & 1 \end{pmatrix},$$

而 $\overline{(-\bar{a}\lambda a)} = -\bar{a}\lambda a$. 如果 $b \neq 0$, 令 $p = \bar{b}\lambda b, q = b^{-1}a$, 则 $\bar{p} = p, \bar{q} = q$. 于是

$$T = \begin{pmatrix} 1+pq & p \\ -qpq & 1-qp \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ -q & 1 \end{pmatrix}\begin{pmatrix} 1 & p \\ 0 & 1 \end{pmatrix}\begin{pmatrix} 1 & 0 \\ q & 1 \end{pmatrix}.$$

因此本定理成立.

系理 设 K_1 是 K 中对称元素所生成之体, 则

$$TU_2\left(K, \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}\right) = TU_2\left(K_1, \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}\right).$$

特别, 如 K 是特征数 $\neq 2$ 的域 Z 上的广义四元数体, 则

$$\begin{aligned} TU_2\left(K, \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}\right) &= TU_2\left(Z, \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}\right) \\ &= Sp_2\left(Z, \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}\right) = SL_2(Z). \end{aligned}$$

又如果 K_1 是域而 K 是 K_1 的二次扩域, 则

$$\begin{aligned} TU_2\left(K, \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}\right) &= TU_2\left(K_1, \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}\right) \\ &= Sp_2\left(K_1, \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}\right) = SL_2(K_1). \end{aligned}$$

定理 2 的证明过程实际上证明了

定理 4 设 $\nu\geqslant 1$, 则 $TU_n(K,H)$ 在 $U_n(K,H)$ 中的中心化子仅由中心矩阵组成, 除开 $n=2$ 而 K 为特征数 $\neq 2$ 的域 Z 上的广义四元数体这个特殊情形. 在后面这一情形, $TU_2\left(K,\begin{pmatrix}0&1\\-1&0\end{pmatrix}\right)$ 在 $U_2\left(K,\begin{pmatrix}0&1\\-1&0\end{pmatrix}\right)$ 中的中心化子由一切矩阵

$$\begin{pmatrix}\lambda&0\\0&\bar{\lambda}^{-1}\end{pmatrix},$$

其中 $\lambda\bar{\lambda}=1$, 所组成.

为了以后的需要, 我们证明次之定理.

定理 5 设 $\nu\geqslant 1$. 设 T 为酉平延, 则有 $U\in TU_n(K,H)$, 使

$$UTU^{-1}=\begin{pmatrix}I^{(\nu)}&[\lambda,0,\cdots,0]&\\&I^{(\nu)}&\\&&I^{(n-2\nu)}\end{pmatrix},$$

而 λ 为 K^* 中某一对称元素.

【证】 依第七章定理 9.1, 有 $U_1\in U_n(K,H)$ 使

$$U_1TU_1^{-1}=\begin{pmatrix}I&[\lambda,0,\cdots,0]&\\&I&\\&&I\end{pmatrix}.$$

我们知道 $TU_n(K,H)$ 是 $U_n(K,H)$ 的正规子群, 故依第七章定理 8.3 及定理 1 可将 U_1 写作

$$U_1=\begin{pmatrix}[a,1,\cdots,1]&&\\&[\bar{a}^{-1},1,\cdots,1]&\\&&I\end{pmatrix}U\qquad(a\neq 0)$$

则

$$UTU^{-1}=\begin{pmatrix}I&[a^{-1}\lambda\bar{a}^{-1},0,\cdots,0]&\\&I&\\&&I\end{pmatrix},$$

其中 $\overline{(a^{-1}\lambda\bar{a}^{-1})}=a^{-1}\lambda\bar{a}^{-1}$. 因此本定理成立.

§3 $PTU_2(K,H)$ 的单性 $(\nu=1)$

在本节中我们要证明次之定理.

定理 1 设 $H = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}$, 则除了下面四个例外情形之外, $PTU_2(K,H)$ 是单群. 例外情形是:

I. 当 $a \to \bar{a}$ 不是 K 的单位自同构时,

$$PTU_2\left(F_4, \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}\right) = PSL_2(F_2),$$

$$PTU_2\left(F_9, \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}\right) = PSL_2(F_3);$$

II. 当 $a \to \bar{a}$ 是 K 的单位自同构时,

$$PTU_2\left(F_2, \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}\right) = PSL_2(F_2),$$

$$PTU_2\left(F_3, \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}\right) = PSL_2(F_3),$$

与这个定理等价的是

定理 2 设 $H = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}$, 则除了四个例外情形之外, $TU_2(K,H)$ 的真正规子群必包含在它的中心 W_2 之中. 四个例外情形就是相应于定理 1 中那四个射影群的酉平延群.

在下面证明定理 2 过程中, 我们同时还证明了次之定理.

定理 3 设 $H = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}$, 并假定 $S \neq F_2$ 或 F_3. 设 $\mathfrak{N}$ 是 $U_2(K,H)$ 的一个子群而且在 $TU_2(K,H)$ 之下不变, 则 $\mathfrak{N}$ 或者包含在 $U_2(K,H)$ 的中心之中, 或者包有 $TU_2(K,H)$.

为了证明定理 2, 我们先证下面几个引理.

引理 1 设 $H = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}$. 设 $\mathfrak{N}$ 是 $U_2(K,H)$ 的子群, 并假设 $\mathfrak{N}$ 在 $TU_2(K,H)$ 之下不变. 如果 $\mathfrak{N}$ 包有一个形如

(1) $$\begin{pmatrix} 1 & \lambda \\ 0 & 1 \end{pmatrix} \quad (\lambda = \bar{\lambda} \neq 0)$$

的元素, 则 $\mathfrak{N}$ 包有一切形为 (1) 的元素. 更进一步, $\mathfrak{N} \supseteq TU_2(K,H)$.

【证】设 $\mathfrak{N}$ 包有

(2) $$\begin{pmatrix} 1 & \lambda_0 \\ 0 & 1 \end{pmatrix} \quad (\bar{\lambda}_0 = \lambda_0 \neq 0).$$

设 Π 是 K 的素域, 则 $\Pi(\lambda_0)$ 是域而对合 $a\to\bar a$ 在 $\Pi(\lambda_0)$ 上诱导出单位自同构. 易见

$$TU_2(\Pi(\lambda_0),H)=SL_2(\Pi(\lambda_0)).$$

因此 $\mathfrak{N}$ 在 $SL_2(\Pi(\lambda_0))$ 之下不变. 令

$$\mathfrak{N}_1=\mathfrak{N}\cap SL_2(\Pi(\lambda_0)),$$

则 $\mathfrak{N}_1$ 为 $SL_2(\Pi(\lambda_0))$ 的正规子群而且包有 (2). 如果 $\Pi(\lambda_0)\neq F_2$ 或 F_3, 则因 $SL_2(\Pi(\lambda_0))$ 没有非中心真正规子群, 故 $\mathfrak{N}_1=SL_2(\Pi(\lambda_0))$, 因此 $\mathfrak{N}_1$ 包有

$$\begin{pmatrix}1&1\\0&1\end{pmatrix}.\tag{3}$$

如 $\Pi(\lambda_0)=F_2$ 或 F_3, 则 $\lambda_0=\pm1$, 因之 $\mathfrak{N}_1$ 包有 $\begin{pmatrix}1&1\\0&1\end{pmatrix}$ 或 $\begin{pmatrix}1&-1\\0&1\end{pmatrix}$. 如 $\mathfrak{N}_1$ 包有 $\begin{pmatrix}1&-1\\0&1\end{pmatrix}$, 则也包有 $\begin{pmatrix}1&-1\\0&1\end{pmatrix}^2=\begin{pmatrix}1&1\\0&1\end{pmatrix}$. 总之 $\mathfrak{N}$ 包有 (3).

设 $\bar\lambda=\lambda\neq0$ 为 K 中任一对称元素, 则 $\Pi(\lambda)$ 亦为域而 $a\to\bar a$ 在 $\Pi(\lambda)$ 上诱导出单位自同构. 易见

$$TU_2(\Pi(\lambda),H)=SL_2(\Pi(\lambda)),$$

因此 $\mathfrak{N}$ 在 $SL_2(\Pi(\lambda))$ 之下不变. 令

$$\mathfrak{N}_2=\mathfrak{N}\cap SL_2(\Pi(\lambda)),$$

则 $\mathfrak{N}_2$ 为 $SL_2(\Pi(\lambda))$ 的正规子群, 而且包有 (3). 如 $\Pi(\lambda)\neq F_2$ 或 F_3, 则因 $SL_2(\Pi(\lambda))$ 没有非中心真正规子群, 故 $\mathfrak{N}_2=SL_2(\Pi(\lambda))$, 因而包有 (1). 如 $\Pi(\lambda)=F_2$ 或 F_3, 则 $\lambda=\pm1$. 如 $\lambda=1,\mathfrak{N}_2$ 已包有 (3). 如 $\lambda=-1$, 则 $\mathfrak{N}_2$ 也包有 $\begin{pmatrix}1&1\\0&1\end{pmatrix}=\begin{pmatrix}1&-1\\0&1\end{pmatrix}^2$. 总之 $\mathfrak{N}$ 包有 (1).

最后, 更因

$$\begin{pmatrix}0&1\\-1&0\end{pmatrix}\begin{pmatrix}1&\lambda\\0&1\end{pmatrix}\begin{pmatrix}0&1\\-1&0\end{pmatrix}^{-1}=\begin{pmatrix}1&0\\-\lambda&1\end{pmatrix},$$

所以 $\mathfrak{N}$ 也包有

$$\begin{pmatrix}1&0\\\mu&1\end{pmatrix},$$

对一切 $\bar\mu=\mu\neq0$. 因此 $\mathfrak{N}$ 包有 $TU_2(K,H)$.

引理 1 就完全证明了.

引理 1 有下面的直接推论.

引理 2　设 $H = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}$. 设 $\mathfrak{N}$ 是 $TU_2(K,H)$ 的一个正规子群. 如 $\mathfrak{N}$ 包有一个形如

$$\begin{pmatrix} 1 & \lambda \\ 0 & 1 \end{pmatrix} \quad (\bar{\lambda} = \lambda \neq 0)$$

的元素, 则 $\mathfrak{N} = TU_2(K,H)$.

引理 3　设 K 不是域, 也不是特征数 $\neq 2$ 的域 Z 上的广义四元数体, $H = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}$ 而 $S \neq F_2, F_3$. 设 $\mathfrak{N}$ 是 $U_2(K,H)$ 的一个子群而且在 $TU_2(K,H)$ 之下不变, 如 $\mathfrak{N}$ 包有一形如

$$\begin{pmatrix} 0 & \beta \\ \gamma & \delta \end{pmatrix} \tag{4}$$

的元素, 则 $\mathfrak{N} \supseteq TU_2(K,H)$.

【证】　由 (4) 为酉矩阵, 故有

$$\begin{pmatrix} 0 & \beta \\ \gamma & \delta \end{pmatrix} = \begin{pmatrix} 0 & \beta \\ -\bar{\beta}^{-1} & \mu\beta \end{pmatrix}, 而\bar{\mu} = \mu.$$

分别考查 $\mu \neq 0$ 及 $\mu = 0$ 这两个情形.

(i) $\mu \neq 0$. 这时对任意 $\bar{\lambda} = \lambda \in K^*, \mathfrak{N}$ 包有

$$\begin{pmatrix} \lambda & \\ & \lambda^{-1} \end{pmatrix}^{-1} \begin{pmatrix} 0 & \beta \\ -\bar{\beta}^{-1} & \mu\beta \end{pmatrix}^{-1} \begin{pmatrix} \lambda & \\ & \lambda^{-1} \end{pmatrix} \begin{pmatrix} 0 & \beta \\ -\bar{\beta}^{-1} & \mu\beta \end{pmatrix}$$
$$= \begin{pmatrix} \lambda^{-1}\bar{\beta}\lambda^{-1}\bar{\beta}^{-1} & \lambda^{-1}\bar{\beta}\lambda^{-1}(\lambda\mu\lambda - \mu)\beta \\ & \lambda\bar{\beta}^{-1}\lambda\beta \end{pmatrix}.$$

我们断言, 存在 $\bar{\lambda} = \lambda \in K^*$, 使 $\lambda\mu\lambda - \mu \neq 0$. 否则, 有

$$\lambda\mu\lambda - \mu = 0, 对一切\bar{\lambda} = \lambda \in K^*.$$

特别, 取 $\lambda = \mu$, 立得 $\mu = \pm 1$. 这时, 对一切 $\bar{\lambda} = \lambda \in K^*$, 就有 $\lambda^2 = 1$; 因而 $\lambda = \pm 1$, 这与 $S \neq F_2, F_3$ 的假设相违. 因此, $\mathfrak{N}$ 包有一个元素

$$\begin{pmatrix} a & b \\ & \bar{a}^{-1} \end{pmatrix} \quad (b \neq 0). \tag{5}$$

由于, 对任意 $\bar{\lambda} = \lambda \in K^*$,

$$\begin{pmatrix} a & b \\ & \bar{a}^{-1} \end{pmatrix}^{-1} \begin{pmatrix} 1 & \lambda \\ & 1 \end{pmatrix}^{-1} \begin{pmatrix} a & b \\ & \bar{a}^{-1} \end{pmatrix} \begin{pmatrix} 1 & \lambda \\ & 1 \end{pmatrix} = \begin{pmatrix} 1 & \lambda - a^{-1}\lambda\bar{a}^{-1} \\ & 1 \end{pmatrix} \in \mathfrak{N}.$$

因此, 若存在 $\bar\lambda=\lambda\in K^*$, 使 $\lambda-a^{-1}\lambda\bar a^{-1}\neq 0$, 则 $\mathfrak{N}$ 包有一个酉平延. 若对一切 $\bar\lambda=\lambda\in K^*$, 恒有 $\lambda-a^{-1}\lambda\bar a^{-1}=0$, 那么取 $\lambda=1$ 则得 $a\bar a=1$. 于是有

$$a\lambda=\lambda a, \text{对一切} \bar\lambda=\lambda\in K.$$

因为 S 生成 K, 故 $a\in Z$. 这时 (5) 可写作

$$\begin{pmatrix} a & a\tau \\ & a \end{pmatrix} \quad (a\in Z, \bar\tau=\tau\neq 0). \tag{6}$$

于是 $\mathfrak{N}$ 包有

$$\begin{pmatrix} \lambda & \\ & \lambda^{-1} \end{pmatrix}\begin{pmatrix} a & a\tau \\ & a \end{pmatrix}\begin{pmatrix} \lambda & \\ & \lambda^{-1} \end{pmatrix}^{-1}\begin{pmatrix} a & a\tau \\ & a \end{pmatrix}^{-1}=\begin{pmatrix} 1 & \lambda\tau\lambda-\tau \\ & 1 \end{pmatrix}, \tag{7}$$

对一切 $\bar\lambda=\lambda\in K^*$. 如果存在 $\bar\lambda=\lambda\in K^*$, 使 $\lambda\tau\lambda-\lambda\neq 0$, 则 $\mathfrak{N}$ 有一个酉平延 (7). 否则由 $\lambda\tau\lambda-\tau=0$ 对一切 $\bar\lambda=\lambda$, 取 $\lambda=\tau$ 立得 $\tau=\pm 1$, 于是有 $\lambda^2=1$, 因而 $\lambda=\pm 1$ 对一切 $\bar\lambda=\lambda$, 这就与 $S\neq F_2, F_3$ 的假设矛盾.

(ii) $\mu=0$. 这时 $\mathfrak{N}$ 包有

$$\begin{pmatrix} 0 & \beta \\ -\bar\beta^{-1} & 0 \end{pmatrix}.$$

对 $\bar\lambda=\lambda\in K^*$, $\begin{pmatrix} 0 & \lambda \\ -\lambda^{-1} & 0 \end{pmatrix}\in TU_2(K,H)$. 因此, $\mathfrak{N}$ 包有

$$\begin{pmatrix} 0 & \lambda \\ -\lambda^{-1} & 0 \end{pmatrix}\begin{pmatrix} & \beta \\ -\bar\beta^{-1} & \end{pmatrix}\begin{pmatrix} & \lambda \\ -\lambda^{-1} & \end{pmatrix}^{-1}\begin{pmatrix} & \beta \\ -\bar\beta^{-1} & \end{pmatrix}^{-1}=\begin{pmatrix} \lambda\bar\beta^{-1}\lambda\beta^{-1} & \\ & \lambda^{-1}\beta\lambda^{-1}\bar\beta \end{pmatrix}.$$

如果有 $\bar\lambda=\lambda$, 使 $\lambda^{-1}\beta\lambda^{-1}\bar\beta=a\notin Z$, 则对 $\bar\mu=\mu$, 有

$$\begin{pmatrix} \bar a^{-1} & \\ & a \end{pmatrix}^{-1}\begin{pmatrix} 1 & \mu \\ & 1 \end{pmatrix}^{-1}\begin{pmatrix} \bar a^{-1} & \\ & a \end{pmatrix}\begin{pmatrix} 1 & \mu \\ & 1 \end{pmatrix}=\begin{pmatrix} 1 & \mu-\bar a\mu a \\ & 1 \end{pmatrix}\in\mathfrak{N}.$$

仿前可证, 有 $\bar\mu=\mu$, 使 $\mu-\bar a\mu a\neq 0$, 故知 $\mathfrak{N}$ 包有一个酉平延.

如果对每个 $\bar\lambda=\lambda$, 恒有 $\lambda^{-1}\beta\lambda^{-1}\bar\beta\in Z$, 特别取 $\lambda=1$ 则得 $\beta\bar\beta=a\in Z$, 且 $\bar a=a$. 这时, 对任何

$$\bar\lambda=\lambda\in Z,\quad \bar\mu=\mu\in Z,$$

我们有

$$\begin{pmatrix} 1 & \\ \mu & 1 \end{pmatrix}\begin{pmatrix} 1 & \\ \lambda & 1 \end{pmatrix}\begin{pmatrix} & \beta \\ -\bar\beta^{-1} & \end{pmatrix}\begin{pmatrix} 1 & \\ \lambda & 1 \end{pmatrix}^{-1}\begin{pmatrix} & \beta \\ -\bar\beta^{-1} & \end{pmatrix}^{-1}\begin{pmatrix} 1 & \\ \mu & 1 \end{pmatrix}^{-1}$$

$$=\begin{pmatrix} 1-\lambda\mu(\beta\bar\beta) & \beta\bar\beta\lambda \\ \lambda-\mu^2\lambda\beta\bar\beta-\lambda^2\mu\beta\bar\beta & 1+\mu\lambda\beta\bar\beta+\lambda^2\beta\bar\beta \end{pmatrix}\in\mathfrak{N}.$$

令 Z_0 表示 Z 中对称元素所成之子域. 我们选取 $\lambda, \mu \in Z_0$, 使 $1-\mu\lambda\beta\bar{\beta}=0$. 于是得

$$\begin{pmatrix} 0 & * \\ * & 2+\lambda^2\beta\bar{\beta} \end{pmatrix} \in \mathfrak{N}.$$

我们进一步断言, 可设 $2+\lambda^2\beta\bar{\beta} \neq 0$

当 $Z_0 = F_2$, 则显然 $\beta\bar{\beta}=1$. 取 $\lambda=\mu=1$ 就满足要求.

当 $Z_0 \neq F_3$ 时, 由于 λ^2 之值不唯一, 故恒存在 $\bar{\lambda}=\lambda \in Z_0$, 使 $2+\lambda^2\beta\bar{\beta} \neq 0$.

当 $Z_0 = F_3$ 时, 如果 $\beta\bar{\beta}=2$, 则取 $\lambda=1$ 就有 $2+2=1\neq 0$.

以上诸情形均归结为 $\mu \neq 0$ 的情形.

当 $Z_0 = F_3$ 而 $\beta\bar{\beta}=1$ 时, $\bar{\beta}^{-1}=\beta$. 于是知

$$\begin{pmatrix} 0 & \beta \\ -\beta & 0 \end{pmatrix} \in \mathfrak{N}.$$

这时 $\mathfrak{N}$ 包有

$$\begin{pmatrix} 1 & \\ 1 & 1 \end{pmatrix}\begin{pmatrix} 0 & \beta \\ -\beta & 0 \end{pmatrix}\begin{pmatrix} 1 & \\ -1 & 1 \end{pmatrix}\begin{pmatrix} 0 & -\beta^{-1} \\ \beta^{-1} & \end{pmatrix} = \begin{pmatrix} 1 & 1 \\ 1 & 2 \end{pmatrix},$$

选取 $\bar{\lambda}=\lambda \notin Z$, 令 $F=Z_0(\lambda)$, 则 F 为域而 $F \neq F_2, F_3$. 有

$$\begin{pmatrix} 1 & 1 \\ 1 & 2 \end{pmatrix} \in U_2(F,H) \subset GL_2(F).$$

令 $\mathfrak{N}_1 = \mathfrak{N} \cap U_2(F,H)$, 则 $\mathfrak{N}_1$ 包有 $\begin{pmatrix} 1 & 1 \\ 1 & 2 \end{pmatrix}$, 且 $\mathfrak{N}_1$ 在 $TU_2(F,H)=SL_2(F)$ 之下不变, 故 $\mathfrak{N}_1 \supseteq SL_2(F)$. 因之, $\mathfrak{N}_1$ 包有一酉平延 $\begin{pmatrix} 1 & 1 \\ & 1 \end{pmatrix}$.

现在我们来证明定理 2. 如果 K 是域, 而 $a \to \bar{a}$ 是 K 的单位自同构, 则

$$TU_2\left(K, \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}\right) = SL_2(K),$$

所以, 这时定理 2 是第二章定理 5.3 的特例. 如果 K 是域而 $a \to \bar{a}$ 不是 K 的单位自同构, 以 K_1 表 K 的对称元素所组成的子域, 则 K 是 K_1 的二次扩域, 而

$$TU_2\left(K, \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}\right) = TU_2\left(K_1, \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}\right) = SL_2(K_1).$$

所以, 这时定理 2 仍是第二章定理 5.3 的特例. 同样, 如 K 是特征数 $\neq 2$ 的域上的广义四元数体, 定理 2 也同样成立.

现在设 K 不是域, 也不是特征数 $\neq 2$ 的域上的广义四元数体. 设 $\mathfrak{N}$ 包有一个非中心元素

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix}. \tag{8}$$

如 $b \neq 0$, 则 $b^{-1}a$ 为对称元素, 于是 $\mathfrak{N}$ 包有

$$\begin{pmatrix} 1 & \\ b^{-1}a & 1 \end{pmatrix}\begin{pmatrix} a & b \\ c & d \end{pmatrix}\begin{pmatrix} 1 & \\ b^{-1}a & 1 \end{pmatrix}^{-1}\begin{pmatrix} 0 & * \\ * & * \end{pmatrix}.$$

因此定理 2 从引理 3 推出. 如果 $c \neq 0$, 同理可证 $\mathfrak{N}$ 包有一个形如 (4) 的元素. 最后设 $b = c = 0$, 则 (8) 成为

$$\begin{pmatrix} a & 0 \\ 0 & \bar{a}^{-1} \end{pmatrix}.$$

于是 $\mathfrak{N}$ 包有

$$\begin{pmatrix} 1 & \lambda \\ 0 & 1 \end{pmatrix}^{-1}\begin{pmatrix} a & 0 \\ 0 & \bar{a}^{-1} \end{pmatrix}^{-1}\begin{pmatrix} 1 & \lambda \\ 0 & 1 \end{pmatrix}\begin{pmatrix} a & 0 \\ 0 & \bar{a}^{-1} \end{pmatrix} = \begin{pmatrix} 1 & a^{-1}\lambda\bar{a}^{-1} - \lambda \\ 0 & 1 \end{pmatrix},$$

对一切 $\bar{\lambda} = \lambda \in K^*$. 如 $a^{-1}\lambda\bar{a}^{-1} - \lambda \neq 0$ 对一个 $\bar{\lambda} = \lambda \in K^*$, 则定理 2 从引理 1 推出. 如 $a^{-1}\lambda\bar{a}^{-1} - \lambda = 0$ 对一切 $\bar{\lambda} = \lambda \in K^*$, 即 $a\lambda\bar{a} = \lambda$ 对一切 $\bar{\lambda} = \lambda$. 取 $\lambda = 1$ 得 $a\bar{a} = 1$, 因之 $a\lambda = \lambda a$ 对一切 $\bar{\lambda} = \lambda$. 因 (8) 不是中心元素, 故 $a \notin Z^*$. 于是依引理 1.1 知, K' 是特征数 $\neq 2$ 的域上的广义四元数体, 而它的中心 $Z = S$. 这时,

$$TU_2\left(K, \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}\right) = TU_2\left(Z, \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}\right),$$

因而化到前一情形去了.

这样定理 2 就完全证明了.

§4 $PTU_n(K,H)$ 的单性 $(\nu \geqslant 1)$

我们有下面的定理:

定理 1 设 $\nu \geqslant 1$, 则除了下面六个例外情形之外, $PTU_n(K,H)$ 是单群; 例外情形是:

I. 当 $a \to \bar{a}$ 不是 K 的单位自同构时,

$$PTU_2\left(F_4, \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}\right) = PSL_2(F_2),$$

$$PTU_2\left(F_9, \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}\right) = PSL_2(F_3),$$

$$PTU_3\left(F_4, \begin{pmatrix} 0 & 1 & \\ 1 & 0 & \\ & & 1 \end{pmatrix}\right);$$

II. 当 $a \to \bar{a}$ 是 K 的单位自同构时 (这时, $PTU_n(K,H)$ 是 $PSp_n(K)$),

$$PTU_2\left(F_2, \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}\right) = PSp_2(F_2) = PSL_2(F_2),$$

$$PTU_2\left(F_3, \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}\right) = PSp_2(F_3) = PSL_2(F_3),$$

$$PTU_4\left(F_2, \begin{pmatrix} 0 & I^{(2)} \\ I^{(2)} & 0 \end{pmatrix}\right) = PSp_4(F_2).$$

与这个定理等价的一个定理是

定理 2　设 $\nu \geqslant 1$, 则除了六个例外情形之外, $TU_n(K,H)$ 的真正规子群必包在它的中心 W_n 之中; 六个例外情形是相应于定理 1 中那六个射影群的酉平延群.

当 $n=2$ 时, 定理 2 在上一节里已经证明. 当 $n \geqslant 3$ 时, 我们可以更一般地证明下面的定理:

定理 3　设 $n \geqslant 3$ 而 $\nu \geqslant 1$, 并设 $\mathfrak{N}$ 为 $U_n(K,H)$ 的子群. 如果 $\mathfrak{N}$ 在 $TU_n(K,H)$ 之下不变, 则 $\mathfrak{N}$ 必含在 $U_n(K,H)$ 的中心之中, 或 $\mathfrak{N}$ 必包有 $TU_n(K,H)$; 但下面两个情形需除外:

I. 当 $a \to \bar{a}$ 不是 K 的单位自同构时,

$$U_3\left(F_4, \begin{pmatrix} 0 & 1 & \\ 1 & 0 & \\ & & 1 \end{pmatrix}\right);$$

II. 当 $a \to \bar{a}$ 是 K 的单位自同构时 (这时 $U_n(K,H) = Sp_n(K)$),

$$U_4\left(F_2, \begin{pmatrix} 0 & I^{(2)} \\ I^{(2)} & 0 \end{pmatrix}\right) = Sp_4(F_2).$$

为了证明定理 3, 先证下面两个引理.

引理 1 设 $\nu \geqslant 1$. 如 $\mathfrak{N}$ 是 $U_n(K,H)$ 的子群, 并假设 $\mathfrak{N}$ 在 $TU_n(K,H)$ 之下不变, 而且包有一个酉平延, 那么 $\mathfrak{N} \supseteq TU_n(K,H)$.

【证】 设 T_0 为酉平延而 $T_0 \in \mathfrak{N}$. 依定理 2.5, 有 $P_0 \in TU_n(K,H)$, 使

$$(1) \qquad P_0T_0P_0^{-1} = \begin{pmatrix} I^{(\nu)} & [\lambda_0, 0, \cdots, 0] & \\ & I^{(\nu)} & \\ & & I \end{pmatrix} \quad (\bar{\lambda}_0 = \lambda_0 \neq 0).$$

因 $\mathfrak{N}$ 在 $TU_n(K,H)$ 之下不变, 故 $\mathfrak{N}$ 包有 (1).

要证 $TU_n(K,H) \subseteq \mathfrak{N}$, 只要能证 $\mathfrak{N}$ 包有一切酉平延即可. 设 T 是任一酉平延, 仍依定理 2.5, 有 $P \in TU_n(K,H)$, 使

$$(2) \qquad PTP^{-1} = \begin{pmatrix} I^{(\nu)} & [\lambda_0, 0, \cdots, 0] & \\ & I^{(\nu)} & \\ & & I \end{pmatrix} \quad (\bar{\lambda} = \lambda \neq 0).$$

如能证 $\mathfrak{N}$ 包有 (2), 则因 $\mathfrak{N}$ 在 $TU_n(K,H)$ 之下不变, 故 $\mathfrak{N}$ 也包有 T. 因此只要证明: 在 $\mathfrak{N}$ 包有 (1) 的假设下, $\mathfrak{N}$ 也包有一切形如 (2) 的元素, 但这是引理 3.1 的推论.

引理 2 设 $\mathfrak{N}$ 是 $U_n(K,H)$ 的子群, 而且在 $TU_n(K,H)$ 之下不变, 则 $\mathfrak{N}$ 在 $U_n(K,H)$ 中的共轭子群也在 $TU_n(K,H)$ 之下不变. 而且, 如果 $\mathfrak{N}$ 在 $U_n(K,H)$ 中的一个共轭子群包有 $TU_n(K,H)$, 则 $\mathfrak{N}$ 亦然.

【证】 设 $R \in U_n(K,H)$, 则 $R^{-1}\mathfrak{N}R$ 为 $\mathfrak{N}$ 在 $U_n(K,H)$ 中的一个共轭子群. 设 $T \in TU_n(K,H)$, 则因 $RT^{-1}R^{-1} \in TU_n(K,H)$,

$$T^{-1}(R^{-1}\mathfrak{N}R)T = R^{-1}(RT^{-1}R^{-1})\mathfrak{N}(RT^{-1}R^{-1})^{-1}R = R^{-1}\mathfrak{N}R.$$

这证明了本引理的第一个断言.

其次, 如 $R^{-1}\mathfrak{N}R \supseteq TU_n(K,H)$, 则

$$\mathfrak{N} \supseteq RTU_n(K,H)R^{-1} = TU_n(K,H),$$

因此第二个断言也成立.

现在我们来证明定理 3. 设 $\mathfrak{N}$ 是 $U_n(K,H)$ 的正规子群, 而且 $\mathfrak{N}$ 在 $TU_n(K,H)$ 之下不变. 如果 $\mathfrak{N}$ 不属于 $U_n(K,H)$ 的中心, 则 $\mathfrak{N}$ 必包有一个非中心元素 N. 因此存在一个酉平延 T, 使

$$T^{-1}N^{-1}TN \neq I.$$

由 $\mathfrak{N}$ 在 $TU_n(K,H)$ 之下的不变性, 更知 $T^{-1}N^{-1}TN \in \mathfrak{N}$.

依第七章定理 9.1, 可设

$$T = I + H\bar{v}'\lambda v,$$

其中 v 为 n 维迷向向量, 即 $vH\bar{v}' = 0$, 而 $\bar{\lambda} = \lambda \neq 0$. 于是

$$N^{-1}TN = I + H\overline{(vN)}'\lambda(vN).$$

考查 $\begin{pmatrix} v \\ vN \end{pmatrix}$. 因 $vH\bar{v}' = 0$, 我们有

$$\begin{pmatrix} v \\ vN \end{pmatrix} H \overline{\begin{pmatrix} v \\ vN \end{pmatrix}}' = \begin{pmatrix} 0 & vH\overline{(vN)}' \\ vNH\bar{v}' & 0 \end{pmatrix}.$$

我们分别以下两种情形进行研究.

(i) $vH\overline{(vN)}' = 0$. 这时 $\begin{pmatrix} v \\ vN \end{pmatrix}$ 是全迷向的. 我们再分以下两种情形进行研究.

(i-1) $\begin{pmatrix} v \\ vN \end{pmatrix}$ 的秩等于 1. 那么 $vN = av, a \neq 0, a \in K$. 于是

$$\begin{aligned} T^{-1}N^{-1}TN =&(I - H\bar{v}'\lambda v)(I + H\overline{(vN)}'\lambda(vN)) \\ =&I - H\bar{v}'\lambda v + H\overline{(vN)}'\lambda(vN) \\ =&I - H\bar{v}'\lambda v + H\overline{av}'\lambda av \\ =&I + H\bar{v}'(\bar{a}\lambda a - \lambda)v. \end{aligned}$$

因 $T^{-1}N^{-1}TN \neq I$, 故 $\bar{a}\lambda a - \lambda \neq 0$, 因之 $T^{-1}N^{-1}TN$ 是个酉平延. 这就证明了 $\mathfrak{N}$ 包有一个酉平延. 由引理 1 知 $\mathfrak{N} \supseteq TU_n(K, H)$.

(i-2) $\begin{pmatrix} v \\ vN \end{pmatrix}$ 的秩等于 2. 于是这时 $\nu \geqslant 2$. 我们注意

$$\begin{pmatrix} 1 & 0 & 0^{(1,n-2)} \\ 0 & 1 & 0^{(1,n-2)} \end{pmatrix} H \begin{pmatrix} 1 & 0 & 0^{(1,n-2)} \\ 0 & 1 & 0^{(1,n-2)} \end{pmatrix}' = \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix},$$

因此依第七章定理 6.1 的系理 2, 有 $R \in U_n(K, H)$, 使

$$\begin{pmatrix} v \\ vN \end{pmatrix} R = \begin{pmatrix} 1 & 0 & 0^{(1,n-2)} \\ 0 & 1 & 0^{(1,n-2)} \end{pmatrix}.$$

令 $\mathfrak{N}_1 = R^{-1}\mathfrak{N}R$, 则 $\mathfrak{N}_1$ 包有

$$R^{-1}T^{-1}N^{-1}TNR = R^{-1}T^{-1}R \cdot R^{-1}N^{-1}TNR.$$

我们有

$$P^{-1}T^{-1}R = I - H\overline{(vR)}'\lambda(vR)$$
$$= I - H(1,0,0^{(1,n-2)})'\lambda(1,0,0^{(1,n-2)})$$
$$= \begin{pmatrix} I^{(\nu)} & & \\ [\lambda,0,\cdots,0] & I^{(\nu)} & \\ & & I \end{pmatrix},$$

$$P^{-1}(T^{-1}TN)R = I + H\overline{(vNR)}'\lambda(vNR)$$
$$= I + H(0,1,0^{(1,n-2)})'\lambda(0,1,0^{(1,n-2)})$$
$$= \begin{pmatrix} I^{(\nu)} & & \\ [0,-\lambda,0,\cdots,0] & I^{(\nu)} & \\ & & I \end{pmatrix}.$$

于是 $\mathfrak{N}_1$ 包有

$$R^{-1}T^{-1}N^{-1}TNR = \begin{pmatrix} I^{(\nu)} & & \\ [\lambda,-\lambda,0,\cdots,0] & I^{(\nu)} & \\ & & I \end{pmatrix}.$$

如能证明 $\mathfrak{N}_1 \supseteq TU_n(K,H)$, 则从引理 2 推出 $\mathfrak{N} \supseteq TU_n(K,H)$.

现在去证明 $\mathfrak{N}_1 \supseteq TU_n(K,H)$. 为书写简便起见, 设 $n = 2\nu = 4$. 于是 $\mathfrak{N}_1$ 包有

$$\begin{pmatrix} I^{(2)} & \\ \begin{pmatrix} -\lambda & 0 \\ 0 & \lambda \end{pmatrix} & I^{(2)} \end{pmatrix}, \text{而} \bar{\lambda} = \lambda \neq 0.$$

我们来证明 $\mathfrak{N}_1$ 包有一个酉平延. 首先, $\mathfrak{N}_1$ 包有

$$\begin{pmatrix} \begin{pmatrix} 1 & \\ -1 & 1 \end{pmatrix} & \\ & \begin{pmatrix} 1 & 1 \\ & 1 \end{pmatrix} \end{pmatrix} \begin{pmatrix} I & \\ \begin{pmatrix} -\lambda & \\ & \lambda \end{pmatrix} & I \end{pmatrix}$$
$$\cdot \begin{pmatrix} \begin{pmatrix} 1 & \\ -1 & 1 \end{pmatrix} & \\ & \begin{pmatrix} 1 & 1 \\ & 1 \end{pmatrix} \end{pmatrix}^{-1} = \begin{pmatrix} I & \\ \begin{pmatrix} 0 & \lambda \\ \lambda & \lambda \end{pmatrix} & I \end{pmatrix}$$

以及

$$\begin{pmatrix} \begin{pmatrix} 1 & \\ & -1 \end{pmatrix} & \\ & \begin{pmatrix} 1 & \\ & -1 \end{pmatrix} \end{pmatrix} \begin{pmatrix} I & & \\ & \begin{pmatrix} 0 & \lambda \\ \lambda & \lambda \end{pmatrix} & \\ & & I \end{pmatrix}$$

$$\cdot \begin{pmatrix} \begin{pmatrix} 1 & \\ & -1 \end{pmatrix} & \\ & \begin{pmatrix} 1 & \\ & -1 \end{pmatrix} \end{pmatrix}^{-1} = \begin{pmatrix} I & & \\ & \begin{pmatrix} 0 & -\lambda \\ -\lambda & \lambda \end{pmatrix} & \\ & & I \end{pmatrix}.$$

如果 K 的特征数 $\neq 2$, 则 $\mathfrak{N}_1$ 包有

$$\begin{pmatrix} I & & \\ & \begin{pmatrix} 0 & \lambda \\ \lambda & \lambda \end{pmatrix} & \\ & & I \end{pmatrix} \begin{pmatrix} I & & \\ & \begin{pmatrix} 0 & -\lambda \\ -\lambda & \lambda \end{pmatrix} & \\ & & I \end{pmatrix} = \begin{pmatrix} I & & \\ & \begin{pmatrix} 0 & 0 \\ 0 & 2\lambda \end{pmatrix} & \\ & & I \end{pmatrix},$$

这是一个酉平延.

今设 K 的特征数 $= 2$. 则 $\mathfrak{N}_1$ 包有

$$\begin{pmatrix} \begin{pmatrix} \alpha & \\ & \alpha^{-1} \end{pmatrix} & \\ & \overline{\begin{pmatrix} \alpha & \\ & \alpha^{-1} \end{pmatrix}}'^{-1} \end{pmatrix} \begin{pmatrix} I & & \\ & \begin{pmatrix} 0 & \lambda \\ \lambda & \lambda \end{pmatrix} & \\ & & I \end{pmatrix}$$

$$\cdot \begin{pmatrix} \begin{pmatrix} \alpha & \\ & \alpha^{-1} \end{pmatrix} & \\ & \overline{\begin{pmatrix} \alpha & \\ & \alpha^{-1} \end{pmatrix}}'^{-1} \end{pmatrix}^{-1} = \begin{pmatrix} I & & \\ & \begin{pmatrix} 0 & \bar{\alpha}^{-1}\lambda\alpha \\ \bar{\alpha}\lambda\alpha^{-1} & \bar{\alpha}\lambda\alpha \end{pmatrix} & \\ & & I \end{pmatrix},$$

于是 $\mathfrak{N}_1$ 包有

$$(3)\quad \begin{pmatrix} I & & \\ & \begin{pmatrix} 0 & \lambda \\ \lambda & \lambda \end{pmatrix} & \\ & & I \end{pmatrix} \begin{pmatrix} I & & \\ & \begin{pmatrix} 0 & \bar{\alpha}^{-1}\lambda\alpha \\ \bar{\alpha}\lambda\alpha^{-1} & \bar{\alpha}\lambda\alpha \end{pmatrix} & \\ & & I \end{pmatrix} = \begin{pmatrix} I & & \\ & \begin{pmatrix} 0 & \lambda + \bar{\alpha}^{-1}\lambda\alpha \\ \lambda + \bar{\alpha}\lambda\alpha^{-1} & \lambda + \bar{\alpha}\lambda\alpha \end{pmatrix} & \\ & & I \end{pmatrix}.$$

如果 $\lambda \neq 1$, 令 $\alpha = \lambda$, (3) 就是一个酉平延. 现在设 $\lambda = 1$. 如果 $S \neq F_2$ 选取 $\alpha \in S, \alpha \neq 0, 1$, 则 $\alpha^2 \neq 1$, 而 (3) 化为酉平延

$$\begin{pmatrix} I & & \\ & \begin{pmatrix} 0 & 0 \\ 0 & 1 + \alpha^2 \end{pmatrix} & \\ & & I \end{pmatrix}.$$

如果 $S=F_2$, 则 $K=F_2$ 或 F_4. 先研究 $K=F_4$ 的情形. 设 $K=F_2(x), x\bar{x}=1, \bar{x}=x+1$. 在 (3) 中选 $\alpha=x$, 则 (3) 化为

$$\begin{pmatrix} I & & \\ & \begin{pmatrix} 0 & x \\ \bar{x} & 0 \end{pmatrix} & \\ & & I \end{pmatrix}.$$

于是 $\mathfrak{N}_1$ 包有

$$\begin{pmatrix} I & & \\ & \begin{pmatrix} 0 & x \\ \bar{x} & 0 \end{pmatrix} & \\ & & I \end{pmatrix}\begin{pmatrix} \begin{pmatrix} 1 & \\ 1 & 1 \end{pmatrix} & \\ & \begin{pmatrix} 1 & 1 \\ & 1 \end{pmatrix} \end{pmatrix}\begin{pmatrix} I & & \\ & \begin{pmatrix} 0 & x \\ \bar{x} & 0 \end{pmatrix} & \\ & & I \end{pmatrix}^{-1}$$

$$\cdot\begin{pmatrix} \begin{pmatrix} 1 & \\ 1 & 1 \end{pmatrix} & \\ & \begin{pmatrix} 1 & 1 \\ & 1 \end{pmatrix} \end{pmatrix}^{-1} = \begin{pmatrix} I & & \\ & \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix} & \\ & & I \end{pmatrix},$$

这是一个酉平延.

如果 $K=F_2$, 这时 n 是 $\geqslant 6$ 的偶数而 $U_n(F_2,H)=Sp_n(F_2)$. 为书写简便起见, 设 $n=6$. 我们已经知道 $\mathfrak{N}_1$ 包有

$$\begin{pmatrix} I & & \\ & \begin{pmatrix} 1 & & \\ & 1 & \\ & & 0 \end{pmatrix} & \\ & & I \end{pmatrix} \text{ 和 } \begin{pmatrix} I & & \\ & \begin{pmatrix} 0 & 1 & \\ 1 & 1 & \\ & & 0 \end{pmatrix} & \\ & & I \end{pmatrix}.$$

于是 $\mathfrak{N}_1$ 包有

$$\begin{pmatrix} \begin{pmatrix} & & 1 \\ & 1 & \\ 1 & & \end{pmatrix} & \\ & \begin{pmatrix} & & 1 \\ & 1 & \\ 1 & & \end{pmatrix} \end{pmatrix}\begin{pmatrix} I & & \\ & \begin{pmatrix} 1 & & \\ & 1 & \\ & & 0 \end{pmatrix} & \\ & & I \end{pmatrix}$$

$$\cdot\begin{pmatrix} \begin{pmatrix} & & 1 \\ & 1 & \\ 1 & & \end{pmatrix} & \\ & \begin{pmatrix} & & 1 \\ & 1 & \\ 1 & & \end{pmatrix} \end{pmatrix}^{-1} = \begin{pmatrix} I & \\ \begin{pmatrix} 0 & & \\ & 1 & \\ & & 1 \end{pmatrix} & I \end{pmatrix}.$$

因之 $\mathfrak{N}_1$ 包有

$$\begin{pmatrix} I & \\ \begin{pmatrix} 0 & 1 & \\ 1 & 1 & \\ & & 0 \end{pmatrix} & I \end{pmatrix}\begin{pmatrix} I & \\ \begin{pmatrix} 0 & & \\ & 1 & \\ & & 1 \end{pmatrix} & I \end{pmatrix} = \begin{pmatrix} I & \\ \begin{pmatrix} 0 & 1 & \\ 1 & 0 & \\ & & 1 \end{pmatrix} & I \end{pmatrix}$$

以及

$$\begin{pmatrix} \begin{pmatrix} 1 & 1 & 1 \\ 1 & 0 & 1 \\ 0 & 1 & 1 \end{pmatrix}^{\prime -1} & \\ & \begin{pmatrix} 1 & 1 & 1 \\ 1 & 0 & 1 \\ 0 & 1 & 1 \end{pmatrix} \end{pmatrix}\begin{pmatrix} I & \\ \begin{pmatrix} 0 & 1 & \\ 1 & 0 & \\ & & 1 \end{pmatrix} & I \end{pmatrix}$$

$$\cdot\begin{pmatrix} \begin{pmatrix} 1 & 1 & 1 \\ 1 & 0 & 1 \\ 0 & 1 & 1 \end{pmatrix}^{\prime -1} & \\ & \begin{pmatrix} 1 & 1 & 1 \\ 1 & 0 & 1 \\ 0 & 1 & 1 \end{pmatrix} \end{pmatrix}^{-1} = \begin{pmatrix} I & \\ I & I \end{pmatrix}.$$

所以 $\mathfrak{N}_1$ 包有

$$\begin{pmatrix} I & \\ I & I \end{pmatrix}\begin{pmatrix} I & \\ \begin{pmatrix} 0 & & \\ & 1 & \\ & & 1 \end{pmatrix} & I \end{pmatrix} = \begin{pmatrix} I & \\ \begin{pmatrix} 1 & & \\ & 0 & \\ & & 0 \end{pmatrix} & I \end{pmatrix},$$

而这是一个酉平延.

(ii) $vH\overline{(vN)}' \neq 0$. 令 $vH\overline{(vH)}' = a$, 则

$$\begin{pmatrix} a^{-1} & 0 \\ 0 & 1 \end{pmatrix}\begin{pmatrix} v \\ vN \end{pmatrix} H \overline{\begin{pmatrix} v \\ vN \end{pmatrix}}' \overline{\begin{pmatrix} a^{-1} & 0 \\ 0 & 1 \end{pmatrix}}' = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}.$$

但是

$$\begin{pmatrix} 1 & 0^{(1,\nu-1)} & 0 & 0 & 0 \\ 0 & 0 & 1 & 0^{(1,\nu-1)} & 0 \end{pmatrix} H \begin{pmatrix} 1 & 0^{(1,\nu-1)} & 0 & 0 & 0 \\ 0 & 0 & 1 & 0^{(1,\nu-1)} & 0 \end{pmatrix}' = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix},$$

故依第七章定理 6.1 的系理 2, 有酉矩阵 R, 使

(4) $$\begin{pmatrix} 1 & 0^{(1,\nu-1)} & 0 & 0 & 0 \\ 0 & 0 & 1 & 0^{(1,\nu-1)} & 0 \end{pmatrix} = \begin{pmatrix} a^{-1} & \\ & 1 \end{pmatrix}\begin{pmatrix} v \\ vN \end{pmatrix} R.$$

只要证明 $\mathfrak{N}_1 = R^{-1}\mathfrak{N}R$ 包有 $TU_n(K,H)$, 就从引理 2 推出

$$\mathfrak{N} \supseteq TU_n(K,H).$$

我们知道 $\mathfrak{N}_1$ 包有

$$R^{(-1)}(T^{-1}N^{-1}TN)R = (R^{-1}T^{-1}R)(R^{-1}N^{-1}TNR).$$

由 (4) 我们有 $vR = (a,0,\cdots,0), vNR = (0^{(1,\nu)},1,0,\cdots,0)$. 因此

$$\begin{aligned} R^{-1}T^{-1}R &= I - H\overline{(vR)}'\lambda(vR) \\ &= \begin{pmatrix} I & & \\ [\bar{a}\lambda a,0,\cdots,0] & I & \\ & & I \end{pmatrix} \end{aligned}$$

以及

$$\begin{aligned} R^{-1}N^{-1}TNR &= I + H\overline{(vNR)}'\lambda(vNR) \\ &= \begin{pmatrix} I & [\lambda,0,\cdots,0] & \\ & I & \\ & & I \end{pmatrix}. \end{aligned}$$

所以

(5) $$R^{-1}(T^{-1}N^{-1}TN)R = \begin{pmatrix} 1 & & \lambda & & \\ & I^{(\nu-1)} & & 0^{(\nu-1)} & \\ \bar{a}\lambda a & & 1+\bar{a}\lambda a\lambda & & \\ & 0^{(\nu-1)} & & I^{(\nu-1)} & \\ & & & & I \end{pmatrix}.$$

由于

$$\begin{pmatrix} 1 & \\ \lambda^{-1} & 1 \end{pmatrix}\begin{pmatrix} 1 & \lambda \\ \bar{a}\lambda a & 1+\bar{a}\lambda a\lambda \end{pmatrix}\begin{pmatrix} 1 & \\ \lambda^{-1} & 1 \end{pmatrix}^{-1} = \begin{pmatrix} 0 & \lambda \\ -\lambda^{-1} & \mu\lambda \end{pmatrix},$$

其中 $\mu = 2\lambda^{-1} + \bar{a}\lambda a \in S$, 所以 $\mathfrak{N}_1$ 包有

$$(6)\qquad \begin{pmatrix} 0 & & \lambda & & \\ & I^{(\nu-1)} & & 0^{(\nu-1)} & \\ -\lambda^{-1} & & \mu\lambda & & \\ & 0^{(\nu-1)} & & I^{(\nu-1)} & \\ & & & & I \end{pmatrix}.$$

如果 $S \neq F_2$ 或 F_3, 则从引理 3.3 推出 $\mathfrak{N}_1$ 包有酉平延. 于是我们的定理就从引理 1 推出.

剩下来还要研究 $S = F_2$ 或 F_3 的情形.

(ii-1) $S = F_2$. 这时 $K = F_2$ 或 F_4. 因 $U_3\left(F_4, \begin{pmatrix} 0 & 1 & \\ 1 & 0 & \\ & & 1 \end{pmatrix}\right)$ 是例外, 所以只需研究 $n \geqslant 4$ 的情形, 而这时一定有 $\nu \geqslant 2$. 以下为书写方便起见, 设 $n = 4$. 这时 (5) 化为

$$\begin{pmatrix} 1 & & 1 & \\ & 1 & & 0 \\ 1 & & 0 & \\ & 0 & & 1 \end{pmatrix}.$$

于是 $\mathfrak{N}_1$ 也包有

$$N_1 = \begin{pmatrix} 0 & 1 & & \\ 1 & 0 & & \\ & & 0 & 1 \\ & & 1 & 0 \end{pmatrix}\begin{pmatrix} 1 & & 1 & \\ & 1 & & 0 \\ 1 & & 0 & \\ & 0 & & 1 \end{pmatrix}$$

$$\cdot \begin{pmatrix} 0 & 1 & & \\ 1 & 0 & & \\ & & 0 & 1 \\ & & 1 & 0 \end{pmatrix}^{-1}\begin{pmatrix} 1 & & 1 & \\ & 1 & & 0 \\ 1 & & 0 & \\ & 0 & & 1 \end{pmatrix} = \begin{pmatrix} I & I \\ I & 0 \end{pmatrix}.$$

令 $v_1 = (1,1,0,0)$, 则

$$T_1 = I + H\bar{v}_1'v_1 = \begin{pmatrix} I & \\ \begin{matrix} 1 & 1 \\ 1 & 1 \end{matrix} & I \end{pmatrix}.$$

注意

$$T_1^{-1}N_1^{-1}T_1N_1 = \begin{pmatrix} I & \\ \begin{matrix} 1 & 1 \\ 1 & 1 \end{matrix} & I \end{pmatrix} \begin{pmatrix} 0 & I \\ I & I \end{pmatrix}$$

$$\cdot \begin{pmatrix} I & \\ \begin{matrix} 1 & 1 \\ 1 & 1 \end{matrix} & I \end{pmatrix} \begin{pmatrix} I & I \\ I & 0 \end{pmatrix} = \begin{pmatrix} 0 & 1 & 1 & 1 \\ 1 & 0 & 1 & 1 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{pmatrix} \neq I^{(4)},$$

$$v_1N_1 = (1,1,1,1).$$

但是

$$v_1H\overline{(v_1N_1)}' = 0,$$

这就化到情形 (i) 去了.

(ii-2) $S = F_3$. 这时 $K = F_3$ 或 F_9. 分别研究这两个情形:

(ii-2-1) $K = F_3$. 这时 $U_n(K,H) = Sp_n(F_3)$, 因之 n 为偶数. 为书写简便起见, 以下设 $n = 4$. 这时 (5) 化为

$$\begin{pmatrix} 1 & & \lambda & \\ & 1 & & 0 \\ \lambda & & -1 & \\ & 0 & & 1 \end{pmatrix}.$$

于是 $\mathfrak{N}_1$ 包有

$$\begin{pmatrix} 1 & & \lambda & \\ & 1 & & 0 \\ \lambda & & -1 & \\ & 0 & & 1 \end{pmatrix}^{-1} = \begin{pmatrix} -1 & & -\lambda & \\ & 1 & & 0 \\ -\lambda & & 1 & \\ & 0 & & 1 \end{pmatrix}.$$

因此 $\mathfrak{N}_1$ 也包有

$$N_2 = \begin{pmatrix} 1 & & \lambda & \\ & 1 & & 0 \\ \lambda & & -1 & \\ & 0 & & 1 \end{pmatrix} \begin{pmatrix} 0 & 1 & & \\ 1 & 0 & & \\ & & 0 & 1 \\ & & 1 & 0 \end{pmatrix}$$

$$\cdot \begin{pmatrix} -1 & & -\lambda & \\ & 1 & & 0 \\ -\lambda & & 1 & \\ & 0 & & 1 \end{pmatrix} \begin{pmatrix} 0 & 1 & & \\ 1 & 0 & & \\ & & 0 & 1 \\ & & 1 & 0 \end{pmatrix}^{-1} = \begin{pmatrix} 1 & & \lambda & \\ & -1 & & -\lambda \\ \lambda & & -1 & \\ & -\lambda & & 1 \end{pmatrix}.$$

令 $v_2 = (1, 1, 0, 0)$, 则

$$v_2 N_2 = (1, -1, \lambda, -\lambda)$$

与 v_2 线性无关. 令

$$T_2 = I + H\bar{v}_2' v_2,$$

则 $N_2 T_2 \neq T_2 N_2$. 注意

$$v_2 H \overline{(v_2 N_2)}' = (1, 1, 0, 0) \begin{pmatrix} 0 & I \\ -I & 0 \end{pmatrix} \begin{pmatrix} 1 \\ -1 \\ \lambda \\ -\lambda \end{pmatrix} = (0\ 0\ 1\ 1) \begin{pmatrix} 1 \\ -1 \\ \lambda \\ -\lambda \end{pmatrix} = 0,$$

这又化到情形 (i) 去了.

(ii-2-2) $K = F_9$. 为书写方便起见, 设 $n = 3$. 于是

$$H = \begin{pmatrix} 0 & 1 & \\ -1 & 0 & \\ & & x \end{pmatrix},$$

而 $\bar{x} = -x$. 因为 $F_9 = F_3(x), x + \bar{x} = 0, x\bar{x} = 1, x$ 适合 $x^2 + 1 = 0$. 这时 (6) 化为

$$\begin{pmatrix} 0 & \lambda & \\ -\lambda & \mu\lambda & \\ & & 1 \end{pmatrix}$$

而 $\mu = -\lambda(1 - a\bar{a})$. 如果 $\mu = 0$, 则 $\mathfrak{N}_1$ 包有

$$\begin{pmatrix} 0 & \lambda & \\ -\lambda & 0 & \\ & & 1 \end{pmatrix}^2 = \begin{pmatrix} -1 & & \\ & -1 & \\ & & 1 \end{pmatrix}.$$

如 $\mu\neq 0$, 则 $a\bar{a}\neq 1$, 于是 $a\bar{a}=-1$, 因之 $\mu=\lambda$. 这时 (6) 化为

$$\begin{pmatrix} 0 & \lambda & \\ -\lambda & 1 & \\ & & 1 \end{pmatrix},$$

因此 $\mathfrak{N}_1$ 也包有

$$\begin{pmatrix} 0 & \lambda & \\ -\lambda & 1 & \\ & & 1 \end{pmatrix}^3=\begin{pmatrix} -1 & & \\ & -1 & \\ & & 1 \end{pmatrix}.$$

于是 $\mathfrak{N}_1$ 包有

$$\begin{pmatrix} -1 & & \\ & -1 & \\ & & 1 \end{pmatrix}^{-1}\begin{pmatrix} 1 & -px\bar{p} & p \\ & 1 & \\ & x\bar{p} & 1 \end{pmatrix}^{-1}\begin{pmatrix} -1 & & \\ & -1 & \\ & & 1 \end{pmatrix}$$

$$\cdot\begin{pmatrix} 1 & -px\bar{p} & p \\ & 1 & \\ & x\bar{p} & 1 \end{pmatrix}=\begin{pmatrix} 1 & -px\bar{p} & -p \\ & 1 & \\ & -x\bar{p} & 1 \end{pmatrix},$$

对一切 $p\in K$. 因之 $\mathfrak{N}$ 包有

$$\begin{pmatrix} 1 & -px\bar{p} & p \\ & 1 & \\ & x\bar{p} & 1 \end{pmatrix}$$

对一切 $p\in K$. 所以 $\mathfrak{N}$ 包有

$$\begin{pmatrix} 1 & -x & 1 \\ & 1 & \\ & x & 1 \end{pmatrix}\begin{pmatrix} 1 & -xx\bar{x} & x \\ & 1 & \\ & x\bar{x} & 1 \end{pmatrix}\begin{pmatrix} 1 & -(1+x)x\overline{(1+x)} & 1+x \\ & 1 & \\ & x\overline{(1+x)} & 1 \end{pmatrix}^{-1}=\begin{pmatrix} 1 & 1 & \\ & 1 & \\ & & 1 \end{pmatrix},$$

而这是一个酉平延. 这时我们的定理从引理 1 推出.

这样, 定理 3 就完全证明了.

§5 群 $U'_n(K,H)$ $(n=2\nu)$

在本节中我们假定 n 是偶数而且 $n=2\nu$. 于是

$$H=\begin{pmatrix} 0 & I^{(\nu)} \\ -I^{(\nu)} & 0 \end{pmatrix}.$$

依第七章定理 7.4, $U_n(K,H)$ 中任一矩阵可表成形状

$$\begin{pmatrix} I & \\ X & I \end{pmatrix}\begin{pmatrix} A & \\ & \bar{A}'^{-1} \end{pmatrix}\begin{pmatrix} I & Y \\ & I \end{pmatrix}\begin{pmatrix} I-J & J \\ -J & I-J \end{pmatrix},$$

其中 $\bar{X}'=X, \bar{Y}'=Y, A$ 可逆, 而 $J^2=J$ 是对角形矩阵, 因此也可表成形状

$$(1)\qquad \begin{pmatrix} A & B \\ C & D \end{pmatrix}\begin{pmatrix} I-J & J \\ -J & I-J \end{pmatrix},$$

其中 A 可逆而 $J^2=J$ 为对角形矩阵. 首先我们证明

定理 1　如果有两种方式将 $U_n(K,H)$ 中一矩阵 Σ 表成形状 (1):

$$(2)\quad \Sigma=\begin{pmatrix} A & B \\ C & D \end{pmatrix}\begin{pmatrix} I-J & J \\ -J & I-J \end{pmatrix}=\begin{pmatrix} A_1 & B_1 \\ C_1 & D_1 \end{pmatrix}\begin{pmatrix} I-J_1 & J_1 \\ -J_1 & I-J_1 \end{pmatrix},$$

其中 A 和 A_1 都是可逆矩阵而 $J^2=J$ 和 $J_1^2=J_1$ 都是对角形矩阵, 则

$$\det A(\det A_1)^{-1} \in S^*C/C,$$

这里 S^* 表 S 中非 0 元素所生成之群, 而 C 表 K^* 的换位子群, S^*C 表由 S^* 和 C 所生成之群, S^*C/C 表 S^*C 对正规子群 C 的商群.

【证】　由 (2) 式得

$$\begin{aligned}\begin{pmatrix} A_1 & B_1 \\ C_1 & D_1 \end{pmatrix}&=\begin{pmatrix} A & B \\ C & D \end{pmatrix}\begin{pmatrix} I-J & J \\ -J & I-J \end{pmatrix}\begin{pmatrix} I-J_1 & -J_1 \\ J_1 & I-J_1 \end{pmatrix}\\&=\begin{pmatrix} A & B \\ C & D \end{pmatrix}\begin{pmatrix} I-J-J_1+2JJ_1 & J-J_1 \\ -(J-J_1) & I-J-J_1+2JJ_1 \end{pmatrix},\end{aligned}$$

于是

$$\begin{aligned}A_1 =&A(I-J-J_1+2JJ_1)-B(J-J_1)\\=&A(I-J-J_1+2JJ_1-A^{-1}B(J-J_1)).\end{aligned}$$

因之

$$\begin{aligned}\det A_1 =&\det A \det(I-J-J_1+2JJ_1-A^{-1}B(J-J_1))\\=&\det A \det(I-J-J_1+2JJ_1-(J-J_1)A^{-1}B(J-J_1)).\end{aligned}$$

因 $A^{-1}B$ 是哈矩阵, 故 $A^{-1}B$ 的主子矩阵亦为哈矩阵. 于是本定理从引理 1.2 推出.

系理　如果将 $U_n(K,H)$ 中一元素 Σ 表成形状 (1), 其中 $\det A \in S^*C/C$, 则 Σ 的任意另一表法亦有此性质.

我们以 $U_n'(K,H)$ 表那些酉矩阵 Σ 的集合, 它们具有性质: 如果将 Σ 表成形状 (1), 则 $\det A \in S^*C/C$.

基于定理 1, 我们可以如下地定义一个从 $U_n(K,H)$ 到 K^*/C 对 S^*C/C 的商群 $(K^*/C)/(S^*C/C)$ 之中的映射 ψ: 首先, 将 $U_n(K,H)$ 中一个矩阵 Σ 表成形状 (1), 那么定义

$$\psi: \quad \Sigma \to (\det A)S^*C/C.$$

下面我们将证明 ψ 是个同态映射. 为此, 我们先证明下面三个引理.

引理 1 设 X,Y,Z 都是 $\nu\times\nu$ 哈矩阵, 则

$$\Sigma=\begin{pmatrix} I & Y \\ & I \end{pmatrix}\begin{pmatrix} I & \\ X & I \end{pmatrix}\begin{pmatrix} I & Z \\ & I \end{pmatrix}\in U_n'(K,H).$$

【证】 我们有

$$\Sigma=\begin{pmatrix} I+YX & (I+YX)Z+Y \\ X & I+XZ \end{pmatrix}.$$

设 Y 的秩为 r, 于是有 $\nu\times\nu$ 可逆矩阵 P 存在, 使

$$PY\bar{P}'=\begin{pmatrix} y & 0 \\ 0 & 0 \end{pmatrix},$$

其中 $y=y^{(r)}$ 为 $r\times r$ 可逆哈矩阵. 不妨设

$$P=\begin{pmatrix} I^{(r)} & 0 \\ \beta & I^{(\nu-r)} \end{pmatrix}P_1,$$

其中 P_1 为置换矩阵, β 为 $(\nu-r)\times r$ 矩阵. 将 $\bar{P}'^{-1}XP^{-1}$ 作与 $PY\bar{P}'$ 同样的分块,

$$\bar{P}'^{-1}XP^{-1}=\begin{pmatrix} x & u \\ \bar{u}' & w \end{pmatrix},\quad \bar{x}'=x,\quad \bar{w}'=w.$$

置

$$\text{(3)}\qquad \Sigma_1=\begin{pmatrix} P & 0 \\ 0 & \bar{P}'^{-1} \end{pmatrix}\Sigma\begin{pmatrix} P & 0 \\ 0 & \bar{P}'^{-1} \end{pmatrix}^{-1}=\begin{pmatrix} A_1 & B_1 \\ C_1 & D_1 \end{pmatrix},$$

则

$$A_1=\begin{pmatrix} I^{(r)}+yx & yu \\ 0 & I^{(\nu-r)} \end{pmatrix},$$

$$B_1=\begin{pmatrix} I^{(r)}+yx & yu \\ 0 & I^{(\nu-r)} \end{pmatrix}PZ\bar{P}'+\begin{pmatrix} y & 0 \\ 0 & 0 \end{pmatrix}.$$

令

$$Q = \begin{pmatrix} y^{-1} & -u \\ 0 & I^{(\nu-r)} \end{pmatrix},$$

则 Q 为 $\nu \times \nu$ 可逆矩阵. 置

$$\Sigma_2 = \begin{pmatrix} Q & 0 \\ 0 & \bar{Q}'^{-1} \end{pmatrix} \Sigma_1 = \begin{pmatrix} A_2 & B_2 \\ C_2 & D_2 \end{pmatrix}, \tag{4}$$

则

$$A_2 = \begin{pmatrix} y^{-1}+x & 0 \\ 0 & I^{(\nu-r)} \end{pmatrix},$$

$$B_2 = \begin{pmatrix} y^{-1}+x & 0 \\ 0 & I^{(\nu-r)} \end{pmatrix} PZ\bar{P}' + \begin{pmatrix} I^{(r)} & 0 \\ 0 & 0 \end{pmatrix}.$$

因 x 和 y 都是哈矩阵, 故 $y^{-1}+x$ 亦然. 设 $y^{-1}+x$ 的秩为 s, 则有 $r \times r$ 可逆矩阵 t 存在, 使

$$t(y^{-1}+x)\bar{t}' = \begin{pmatrix} 0 & 0 \\ 0 & z \end{pmatrix},$$

其中 z 为 $s \times s$ 可逆哈矩阵. 不妨设

$$t = \begin{pmatrix} I^{(r-s)} & \alpha \\ & I^{(s)} \end{pmatrix} t_1,$$

其中 t_1 为 $r \times r$ 置换矩阵而 a 为 $(r-s) \times s$ 矩阵. 令

$$T = \begin{pmatrix} t & \\ & I^{(\nu-r)} \end{pmatrix},$$

则 T 为 $\nu \times \nu$ 可逆矩阵. 置

$$\Sigma_3 = \begin{pmatrix} T & \\ & \bar{T}'^{-1} \end{pmatrix} \Sigma_2 \begin{pmatrix} \bar{T}' & \\ & T^{-1} \end{pmatrix} = \begin{pmatrix} A_3 & B_3 \\ C_3 & D_3 \end{pmatrix}, \tag{5}$$

则

$$A_3 = \begin{pmatrix} 0 & & \\ & z^{(s)} & \\ & & I^{(\nu-r)} \end{pmatrix},$$

$$B_3=\begin{pmatrix}0&&\\&z^{(s)}&\\&&I^{(\nu-r)}\end{pmatrix}\bar{T}'^{-1}PZ\bar{P}'T^{-1}+\begin{pmatrix}I^{(r)}&0\\0&0^{(\nu-r)}\end{pmatrix}$$
$$=\begin{pmatrix}I^{(r-s)}&0^{(r-s,s)}&0^{(r-s,\nu-r)}\\&*&\end{pmatrix}.$$

令

$$J=\begin{pmatrix}I^{(r-s)}&\\&0^{(\nu-r+s)}\end{pmatrix},$$

置

(6) $$\Sigma_4=\Sigma_3\begin{pmatrix}I-J&-J\\J&I-J\end{pmatrix}=\begin{pmatrix}A_4&B_4\\C_4&D_4\end{pmatrix},$$

则

$$A_4=A_3(I-J)+B_3J=\begin{pmatrix}I^{(r-s)}&0&0\\ *&z^{(s)}&0\\ *&0&I^{(\nu-r)}\end{pmatrix}.$$

因 z 为 $s\times s$ 可逆哈矩阵, 故依引理 1.2 有

$$\det A_4=\det z^{(s)}\in S^*C/C.$$

从 (3), (4), (5), (6) 推出

$$\Sigma=\begin{pmatrix}P&\\&\bar{P}'^{-1}\end{pmatrix}^{-1}\begin{pmatrix}Q&\\&\bar{Q}'^{-1}\end{pmatrix}^{-1}\begin{pmatrix}T&\\&\bar{T}'^{-1}\end{pmatrix}^{-1}\cdot$$
$$\cdot\Sigma_4\begin{pmatrix}I-J&J\\-J&I-J\end{pmatrix}\begin{pmatrix}\bar{T}'&\\&\bar{T}^{-1}\end{pmatrix}^{-1}\begin{pmatrix}P&\\&\bar{P}'^{-1}\end{pmatrix}$$
$$=\begin{pmatrix}(TQP)^{-1}&\\&\overline{(TQP)}'\end{pmatrix}\begin{pmatrix}A_4&B_4\\C_4&D_4\end{pmatrix}\begin{pmatrix}I-J&J\\-J&I-J\end{pmatrix}\cdot$$
$$\cdot\begin{pmatrix}\bar{T}'^{-1}&\\&T\end{pmatrix}\begin{pmatrix}P&\\&\bar{P}'^{-1}\end{pmatrix}.$$

因为

$$T=\begin{pmatrix}t&0\\0&I^{(\nu-r)}\end{pmatrix},\quad t=\begin{pmatrix}I^{(r-s)}&\alpha\\&I^{(s)}\end{pmatrix}t_1,$$

其中 t_1 为置换矩阵, 所以

$$\begin{pmatrix} I-J & J \\ -J & I-J \end{pmatrix}\begin{pmatrix} \bar{T}'^{-1} & \\ & T \end{pmatrix}$$

$$=\begin{pmatrix} I^{(\nu)} & \begin{pmatrix} 0 & \alpha & \\ \bar{\alpha}' & 0 & \\ & & 0^{(\nu-r)} \end{pmatrix} \\ & I^{(\nu)} \end{pmatrix}\begin{pmatrix} t_1 & 0 & & \\ 0 & I^{(\nu-r)} & & \\ & & \bar{t}_1'^{-1} & 0 \\ & & 0 & I^{(\nu-r)} \end{pmatrix}\begin{pmatrix} I-J_1 & & J_1 & \\ & I^{(\nu-r)} & & \\ -J_1 & & I-J_1 & \\ & & & I^{(\nu-r)} \end{pmatrix},$$

其中

$$J_1=\overline{t_1}'^{-1}\begin{pmatrix} I^{(r-s)} & \\ & 0^{(s)} \end{pmatrix}t_1.$$

又因为

$$P=\begin{pmatrix} I^{(r)} & 0 \\ \beta & I^{(\nu-r)} \end{pmatrix}P_1,$$

其中 P_1 为置换矩阵, 所以

$$\begin{pmatrix} I-J_1 & & J_1 & \\ & I^{(\nu-r)} & & 0 \\ -J_1 & & I-J_1 & \\ & 0 & & I^{(\nu-r)} \end{pmatrix}\begin{pmatrix} P & \\ & \bar{P}'^{-1} \end{pmatrix}=\begin{pmatrix} I^{(r)} & 0 & 0 & -J_1\bar{\beta}' \\ \beta(I-J_1) & I^{(\nu-r)} & -\beta J_1 & 0 \\ & & I^{(r)} & -(I-J_1)\bar{\beta}' \\ & & & I^{(\nu-r)} \end{pmatrix}$$

$$\cdot\begin{pmatrix} P_1 & \\ & \overline{P_1}'^{-1} \end{pmatrix}\begin{pmatrix} I-J_2 & J_2 \\ -J_2 & I-J_2 \end{pmatrix},$$

其中

$$J_2=\overline{P_1}'^{-1}\begin{pmatrix} J_1 & 0 \\ 0 & 0 \end{pmatrix}P_1.$$

因此, 如果写

$$\Sigma=\begin{pmatrix} A & B \\ C & D \end{pmatrix}\begin{pmatrix} I-J_2 & J_2 \\ -J_2 & I-J_2 \end{pmatrix},$$

则

$$A=(TQP)^{-1}A_4\begin{pmatrix} t_1 & \\ & I^{(\nu-r)} \end{pmatrix}\begin{pmatrix} I^{(r)} & \\ \beta(I-J_1) & I^{(\nu-r)} \end{pmatrix}P_1.$$

由于

$$\det T=C,\quad \det P=C,\quad \det Q=\det y^{-1}\in S^*C/C,$$

$$\det t_1 = C,\ \det P_1 = C,\ \det A_4 = \det z \in S^*C/C,$$

所以

$$\det A \in S^*C/C.$$

因此 $\Sigma \in U'_n(K,H)$. 这样引理 1 就证明了.

引理 2 设 A 为 $\nu\times\nu$ 可逆矩阵. 设

$$1 \leqslant i_1 < \cdots < i_r \leqslant \nu,\quad 1 \leqslant i_{r+1} < \cdots < i_\nu \leqslant \nu,$$
$$1 \leqslant j_1 < \cdots < j_r \leqslant \nu,\quad 1 \leqslant j_{r+1} < \cdots < j_\nu \leqslant \nu$$

而且 $i_1, \cdots, i_r, i_{r+1}, \cdots, i_\nu$ 及 $j_1, \cdots, j_r, j_{r+1}, \cdots, j_\nu$ 皆 $1, \cdots, \nu$ 的排列. 以 $A\begin{pmatrix} i_1\cdots i_r \\ j_1\cdots j_r \end{pmatrix}$ 表 A 中位于 (i_k, j_l) $(k,l=1,\cdots,r)$ 处的元素所组成的子矩阵, 对 $\bar{A}'^{-1}\begin{pmatrix} i_{r+1}\cdots i_\nu \\ j_{r+1}\cdots j_\nu \end{pmatrix}$ 亦有同样的意义. 设

$$\det A\begin{pmatrix} i_1\cdots i_r \\ j_1\cdots j_r \end{pmatrix} \neq 0,$$

则

$$\det A\begin{pmatrix} i_1\cdots i_r \\ j_1\cdots j_r \end{pmatrix}\det \bar{A}'^{-1}\begin{pmatrix} j_{r+1}\cdots i_\nu \\ j_{r+1}\cdots j_\nu \end{pmatrix}(\det A)^{-1} \in S^*C/C.$$

特别, 如 $\det A \in S^*C/C$, 则

$$\det A\begin{pmatrix} i_1\cdots i_r \\ j_1\cdots j_r \end{pmatrix}\det \bar{A}'^{-1}\begin{pmatrix} i_{r+1}\cdots i_\nu \\ j_{r+1}\cdots j_\nu \end{pmatrix} \in S^*C/C.$$

【证】 设 P 和 Q 是置换矩阵, 使 $B=PAQ$ 的 $1,2,\cdots,r,r+1,\cdots,\nu$ 行依次为 A 的 $i_1,\cdots,i_r,i_{r+1},\cdots,i_\nu$ 行, 而 B 的 $1,2,\cdots,r,r+1,\cdots,\nu$ 列依次为 A 的 $j_1,\cdots,j_r,j_{r+1},\cdots,j_\nu$ 列. 设

$$B = \begin{pmatrix} A_1 & B_1 \\ C_1 & D_1 \end{pmatrix},\quad A_1 = A_1^{(r)},\quad B_1 = B_1^{(r,\nu-r)}\text{等}.$$

则

$$A_1 = A\begin{pmatrix} i_1\cdots i_r \\ j_1\cdots j_r \end{pmatrix}.$$

由于

$$\begin{pmatrix} A_1 & B_1 \\ C_1 & D_1 \end{pmatrix} = \begin{pmatrix} I & \\ C_1 A_1^{-1} & I \end{pmatrix} \begin{pmatrix} A_1 & B_1 \\ & D_1 - C_1 A_1^{-1} B_1 \end{pmatrix},$$

所以

$$\bar{B}'^{-1} = \begin{pmatrix} I & -\bar{A}_1'^{-1}\bar{C}_1' \\ & I \end{pmatrix} \begin{pmatrix} \bar{A}_1'^{-1} & 0 \\ * & \overline{(D_1 - C_1 A_1^{-1} B_1)}'^{-1} \end{pmatrix}$$

$$= \begin{pmatrix} * & * \\ * & \overline{(D_1 - C_1 A_1^{-1} B_1)}'^{-1} \end{pmatrix}.$$

由于 $B = PAQ$, 所以 $\bar{B}'^{-1} = P\bar{A}'^{-1}Q$, 因此

$$\bar{B}'^{-1} \begin{pmatrix} r+1 \cdots \nu \\ r+1 \cdots \nu \end{pmatrix} = \bar{A}'^{-1} \begin{pmatrix} i_{r+1} \cdots i_\nu \\ j_{r+1} \cdots j_\nu \end{pmatrix}.$$

因之

$$\begin{aligned} &\det A \begin{pmatrix} i_1 \cdots i_r \\ j_1 \cdots j_r \end{pmatrix} \det \bar{A}'^{-1} \begin{pmatrix} i_{r+1} \cdots i_\nu \\ j_{r+1} \cdots j_\nu \end{pmatrix} \\ =& \det A_1 \det \overline{(D_1 - C_1 A_1^{-1} B_1)}'^{-1} \\ =& \det A_1 \det(D_1 - C_1 A_1^{-1} B_1)[\det(D_1 - C_1 A_1^{-1} B_1)]^{-1} \\ &\cdot [\det \overline{(D_1 - C_1 A_1^{-1} B_1)}']^{-1}. \end{aligned}$$

注意到

$$\begin{aligned} &[\det(D_1 - C_1 A_1^{-1} B_1)]^{-1} [\det \overline{(D_1 - C_1 A_1^{-1} B_1)}']^{-1} \\ =& \{\det(D_1 - C_1 A_1^{-1} B_1) \overline{(D_1 - C_1 A_1^{-1} B_1)}'\}^{-1} \in S^* C/C \end{aligned}$$

以及

$$\det A S^* C/C = \det B S^* C/C = \det A_1 \det(D_1 - C_1 A_1^{-1} B_1) S^* C/C,$$

所以

$$\det A \begin{pmatrix} i_1 \cdots i_r \\ j_1 \cdots j_r \end{pmatrix} \det \bar{A}'^{-1} \begin{pmatrix} i_{r+1} \cdots i_\nu \\ j_{r+1} \cdots j_\nu \end{pmatrix} (\det A)^{-1} \in S^* C/C.$$

引理 3　设 $J^2 = J$ 和 $J_1^2 = J_1$ 皆是对角形矩阵. 可以表

$$\begin{pmatrix} I - J & J \\ -J & I - J \end{pmatrix} \begin{pmatrix} I - J_1 & J_1 \\ -J_1 & I - J_1 \end{pmatrix} = \begin{pmatrix} A & 0 \\ 0 & \bar{A}'^{-1} \end{pmatrix} \begin{pmatrix} I - J_2 & J_2 \\ -J_2 & I - J_2 \end{pmatrix},$$

其中 $\det A \in S^*C/C$ 而 $J_2^2=J_2$ 也是对角形矩阵.

【证】 我们有

$$\Sigma = \begin{pmatrix} I-J & J \\ -J & I-J \end{pmatrix}\begin{pmatrix} I-J_1 & J_1 \\ -J_1 & I-J_1 \end{pmatrix} = \begin{pmatrix} I-J-J_1 & J+J_1-2JJ_1 \\ -(J+J_1-2JJ_1) & I-J-J_1 \end{pmatrix}.$$

令 $J_2=J+J_1-2JJ_1$, 则

$$\Sigma = \begin{pmatrix} I-2JJ_1 & \\ & I-2JJ_1 \end{pmatrix}\begin{pmatrix} I-J_2 & J_2 \\ -J_2 & I-J_2 \end{pmatrix}.$$

取 $A=I-2JJ_1$ 即得出引理 3.

基于上面三条引理, 我们可以依次推出以下诸事实 (以下 $J, J_1, \cdots$ 皆表对角形幂等矩阵):

(i) 设 A 为 $\nu\times\nu$ 可逆矩阵, 写

$$\begin{pmatrix} I-J & J \\ -J & I-J \end{pmatrix}\begin{pmatrix} A & \\ & \bar{A}'^{-1} \end{pmatrix}\begin{pmatrix} A_1 & B_1 \\ C_1 & D_1 \end{pmatrix}\begin{pmatrix} I-J_1 & J_1 \\ -J_1 & I-J_1 \end{pmatrix}, \tag{7}$$

其中 A_1 可逆, 则 $(\det A)(\det A_1)^{-1}\in S^*C/C$. 特别, 如 $\det A\in S^*C/C$, 则 (7) 属于 $U'_n(K,H)$.

【证】 将 (7) 式写作

$$\begin{pmatrix} A_1 & B_1 \\ C_1 & D_1 \end{pmatrix}\begin{pmatrix} I-J & J \\ -J & I-J \end{pmatrix}\begin{pmatrix} A & \\ & \bar{A}'^{-1} \end{pmatrix}\begin{pmatrix} I-J_1 & -J_1 \\ J_1 & I-J_1 \end{pmatrix},$$

比较上式 (1,1) 位置的矩阵块, 得出

$$A_1=(I-J)A(I-J_1)+J\bar{A}'^{-1}J_1.$$

于是

$$\det A_1=\det[(I-J)A(I-J_1)+J\bar{A}'^{-1}J_1].$$

依行列式的展开定理及引理 2, 推出

$$\det A_1(\det A)^{-1}\in S^*C/C,$$

因之

$$\det A(\det A_1)^{-1}\in S^*C/C.$$

(ii) 设 $\bar{Y}' = Y$, 则

$$\Sigma = \begin{pmatrix} I-J & J \\ -J & I-J \end{pmatrix} \begin{pmatrix} I & Y \\ & I \end{pmatrix} \in U_n'(K,H).$$

【证】 写

$$\Sigma = \begin{pmatrix} I-J & (I-J)Y+J \\ -J & -JY+I-J \end{pmatrix} \begin{pmatrix} I-J & -J \\ J & I-J \end{pmatrix} \begin{pmatrix} I-J & J \\ -J & I-J \end{pmatrix}$$
$$= \begin{pmatrix} I+(I-J)YJ & * \\ * & * \end{pmatrix} \begin{pmatrix} I-J & J \\ -J & I-J \end{pmatrix}.$$

显然

$$\det[I+(I-J)YJ] = C,$$

因此

$$\Sigma \in U_n'(K,H).$$

(iii) 设 $\bar{X}' = X$, 则

$$\Sigma = \begin{pmatrix} I-J & J \\ -J & I-J \end{pmatrix} \begin{pmatrix} I & \\ X & I \end{pmatrix} \in U_n'(K,H).$$

【证】 写

$$\Sigma = \begin{pmatrix} I-J+JX & J \\ -J+(I-J)X & I-J \end{pmatrix} \begin{pmatrix} I-J & -J \\ J & I-J \end{pmatrix} \begin{pmatrix} I-J & J \\ -J & I-J \end{pmatrix}$$
$$= \begin{pmatrix} I+JX(I-J) & * \\ * & * \end{pmatrix} \begin{pmatrix} I-J & J \\ -J & I-J \end{pmatrix},$$

显然

$$\det[I+JX(I-J)] = C,$$

故 $\Sigma \in U_n'(K,H)$.

(iv) 设

$$\Sigma = \begin{pmatrix} A & B \\ C & D \end{pmatrix}, \quad \Sigma_1 = \begin{pmatrix} A_1 & B_1 \\ C_1 & D_1 \end{pmatrix}$$

是两个酉矩阵而 A 和 A_1 皆可逆. 写

$$\Sigma_2 = \Sigma\Sigma_1 = \begin{pmatrix} A & B \\ C & D \end{pmatrix} \begin{pmatrix} A_1 & B_1 \\ C_1 & D_1 \end{pmatrix} = \begin{pmatrix} A_2 & B_2 \\ C_2 & D_2 \end{pmatrix} \begin{pmatrix} I-J & J \\ -J & I-J \end{pmatrix},$$

则 $\det A\det A_1(\det A_2)^{-1}\in S^*C/C$. 特别, 如果 $\Sigma,\Sigma_1\in U'_n(K,H)$, 则 $\Sigma_2\in U'_n(K,H)$.

【证】 表

$$\Sigma=\begin{pmatrix}A&0\\0&\bar{A}'^{-1}\end{pmatrix}\begin{pmatrix}I&\\X&I\end{pmatrix}\begin{pmatrix}I&Y\\&I\end{pmatrix},$$

$$\Sigma_1=\begin{pmatrix}A_1&0\\0&\overline{A_1}'^{-1}\end{pmatrix}\begin{pmatrix}I&\\X_1&I\end{pmatrix}\begin{pmatrix}I&Y_1\\&I\end{pmatrix},$$

其中 X,Y,X_1,Y_1 都是哈矩阵, 则

$$\Sigma\Sigma_1=\begin{pmatrix}A&0\\0&\bar{A}'^{-1}\end{pmatrix}\begin{pmatrix}A_1&0\\0&\overline{A_1}'^{-1}\end{pmatrix}\begin{pmatrix}I&\\X_2&I\end{pmatrix}$$
$$\cdot\begin{pmatrix}I&Y_2\\&I\end{pmatrix}\begin{pmatrix}I&\\X_1&I\end{pmatrix}\begin{pmatrix}I&Y_1\\&I\end{pmatrix},$$

其中 $Y_2=A_1^{-1}Y\overline{A_1}'^{-1},X_2=\overline{A_1}'XA_1$. 于是由引理 1 即可推出 (iv).

(v) 设

$$\Sigma=\begin{pmatrix}A&B\\C&D\end{pmatrix}\in U_n(K,H),$$

而 A 可逆. 写

$$\Sigma^{-1}=\begin{pmatrix}A_1&B_1\\C_1&D_1\end{pmatrix}\begin{pmatrix}I-J_1&J_1\\-J_1&I-J_1\end{pmatrix},$$

其中 A 可逆, 则 $\det A\ \det A_1\in S^*C/C$. 特别, 如果 $\Sigma\in U'_n(K,H)$, 则 Σ^{-1} 亦然.

【证】 我们有

$$I=\Sigma\Sigma^{-1}=\begin{pmatrix}A&B\\C&D\end{pmatrix}\begin{pmatrix}A_1&B_1\\C_1&D_1\end{pmatrix}\begin{pmatrix}I-J_1&J_1\\-J_1&I-J_1\end{pmatrix}$$

于是 (v) 由 (iv) 及引理 3 推出.

(vi) 设

$$\Sigma=\begin{pmatrix}A&B\\C&D\end{pmatrix}\in U_n(K,H).$$

表

$$\Sigma_1=\begin{pmatrix}I-J&J\\-J&I-J\end{pmatrix}\begin{pmatrix}A&B\\C&D\end{pmatrix}=\begin{pmatrix}A_1&B_1\\C_1&D_1\end{pmatrix}\begin{pmatrix}I-J_1&J_1\\-J_1&I-J_1\end{pmatrix},$$

则 $\det A(\det A_1)^{-1} \in S^*C/C$. 特别, 如 $\Sigma \in U_n'(K,H)$, 则 Σ_1 亦然.

【证】 写

$$\begin{pmatrix} A & B \\ C & D \end{pmatrix} = \begin{pmatrix} A & \\ & \bar{A}'^{-1} \end{pmatrix} \begin{pmatrix} I & \\ X & I \end{pmatrix} \begin{pmatrix} I & Y \\ & I \end{pmatrix}.$$

于是

$$\begin{aligned}
\Sigma_1 &= \begin{pmatrix} I-J & J \\ -J & I-J \end{pmatrix} \begin{pmatrix} A & \\ & \bar{A}'^{-1} \end{pmatrix} \begin{pmatrix} I & \\ X & I \end{pmatrix} \begin{pmatrix} I & Y \\ & I \end{pmatrix} \\
&= \begin{pmatrix} A_2 & B_2 \\ C_2 & D_2 \end{pmatrix} \begin{pmatrix} I-J_2 & J_2 \\ -J_2 & I-J_2 \end{pmatrix} \begin{pmatrix} I & \\ X & I \end{pmatrix} \begin{pmatrix} I & Y \\ & I \end{pmatrix} & (\text{根据 (i)}) \\
&= \begin{pmatrix} A_2 & B_2 \\ C_2 & D_2 \end{pmatrix} \begin{pmatrix} A_3 & B_3 \\ C_3 & D_3 \end{pmatrix} \begin{pmatrix} I-J_2 & J_2 \\ -J_2 & I-J_2 \end{pmatrix} \begin{pmatrix} I & Y \\ & I \end{pmatrix} & (\text{根据 (iii)}) \\
&= \begin{pmatrix} A_4 & B_4 \\ C_4 & D_4 \end{pmatrix} \begin{pmatrix} I-J_3 & J_3 \\ -J_3 & I-J_3 \end{pmatrix} \begin{pmatrix} I-J_2 & J_2 \\ -J_2 & I-J_2 \end{pmatrix} \begin{pmatrix} I & Y \\ & I \end{pmatrix} & (\text{根据 (iv)}) \\
&= \begin{pmatrix} A_4 & B_4 \\ C_4 & D_4 \end{pmatrix} \begin{pmatrix} A_5 & \\ & \overline{A_5}'^{-1} \end{pmatrix} \begin{pmatrix} I-J_4 & J_4 \\ -J_4 & I-J_4 \end{pmatrix} \begin{pmatrix} I & Y \\ & I \end{pmatrix} & (\text{根据引理 3}) \\
&= \begin{pmatrix} A_6 & B_6 \\ C_6 & D_6 \end{pmatrix} \begin{pmatrix} A_7 & B_7 \\ C_7 & D_7 \end{pmatrix} \begin{pmatrix} I-J_4 & J_4 \\ -J_4 & I-J_4 \end{pmatrix} & (\text{根据 (ii)}) \\
&= \begin{pmatrix} A_8 & B_8 \\ C_8 & D_8 \end{pmatrix} \begin{pmatrix} I-J_5 & J_5 \\ -J_5 & I-J_5 \end{pmatrix} \begin{pmatrix} I-J_4 & J_4 \\ -J_4 & I-J_4 \end{pmatrix} & (\text{根据 (iv)}) \\
&= \begin{pmatrix} A_9 & B_9 \\ C_9 & D_9 \end{pmatrix} \begin{pmatrix} I-J_6 & J_6 \\ -J_6 & I-J_6 \end{pmatrix} & (\text{根据引理 3}),
\end{aligned}$$

其中 $J_2, J_3, \cdots, J_6$ 皆是对角形幂等矩阵, 而 $A_2, A_3, \cdots, A_9$ 皆是可逆矩阵, 并有性质

$$\begin{aligned}
&\det A(\det A_2)^{-1} \in S^*C/C, && \det A_3 = C, \\
&\det A_2 \det A_3(\det A_4)^{-1} \in S^*C/C, && \det A_5 = C, \\
&\det A_6 = \det A_4 \det A_5 = \det A_4, && \det A_7 = C, \\
&\det A_6 \det A_7(\det A_8)^{-1} \in S^*C/C, && \det A_9 = \det A_8.
\end{aligned}$$

因此

$$\det A(\det A_9)^{-1} \in S^*C/C.$$

可是根据定理 1, $\det A_1(\det A_9)^{-1} \in S^*C/C$, 所以

$$\det A(\det A_1)^{-1} \in S^*C/C.$$

因此 (vi) 成立.

基于以上诸事实, 我们可以证明

定理 2 设 $\Sigma \in U_n(K,H)$, 表

$$\Sigma = \begin{pmatrix} A & B \\ C & D \end{pmatrix} \begin{pmatrix} I-J & J \\ -J & I-J \end{pmatrix}, \tag{1}$$

其中 A 可逆而 $J^2=J$ 为对角形矩阵. 则从 $U_n(K,H)$ 到

$$(K^*/C)/(S^*C/C)$$

之中的映射

$$\psi: \quad \Sigma \to (\det A)S^*C/C$$

不依赖于 Σ 的特殊表法. 更进一步, 这个映射是从 $U_n(K,H)$ 到

$$(K^*/C)/(S^*C/C)$$

之上的同态映射, 而 $U'_n(K,H)$ 是它的核, 于是

$$U_n(K,H)/U'_n(K,H) \approx (K^*/C)/(S^*C)/C \approx K^*/S^*C.$$

【证】 根据定理 1, 知映射 ψ 不依赖于 Σ 的特殊表法 (1). 这个映射是映上的这一点是显然的. 现在来证它是个同态. 设

$$\Sigma_1 = \begin{pmatrix} A_1 & B_1 \\ C_1 & D_1 \end{pmatrix} \begin{pmatrix} I-J_1 & J_1 \\ -J_1 & I-J_1 \end{pmatrix},$$

其中 A_1 可逆而 $J_1^2=J_1$ 为对角形矩阵. 则

$$\begin{aligned}
\Sigma\Sigma_1 &= \begin{pmatrix} A & B \\ C & D \end{pmatrix}\begin{pmatrix} I-J & J \\ -J & I-J \end{pmatrix}\begin{pmatrix} A_1 & B_1 \\ C_1 & D_1 \end{pmatrix}\begin{pmatrix} I-J_1 & J_1 \\ -J_1 & I-J_1 \end{pmatrix} \\
&= \begin{pmatrix} A & B \\ C & D \end{pmatrix}\begin{pmatrix} A_2 & B_2 \\ C_2 & D_2 \end{pmatrix}\begin{pmatrix} I-J_2 & J_2 \\ -J_2 & I-J_2 \end{pmatrix}\begin{pmatrix} I-J_1 & J_1 \\ -J_1 & I-J_1 \end{pmatrix} \quad (\text{根据 (vi)}) \\
&= \begin{pmatrix} A & B \\ C & D \end{pmatrix}\begin{pmatrix} A_3 & B_3 \\ C_3 & D_3 \end{pmatrix}\begin{pmatrix} I-J_3 & J_3 \\ -J_3 & I-J_3 \end{pmatrix} \quad (\text{根据引理 3}) \\
&= \begin{pmatrix} A_4 & B_4 \\ C_4 & D_4 \end{pmatrix}\begin{pmatrix} I-J_4 & J_4 \\ -J_4 & I-J_4 \end{pmatrix}\begin{pmatrix} I-J_3 & J_3 \\ -J_3 & I-J_3 \end{pmatrix} \quad (\text{根据 (iv)}) \\
&= \begin{pmatrix} A_5 & B_5 \\ C_5 & D_5 \end{pmatrix}\begin{pmatrix} I-J_5 & J_5 \\ -J_5 & I-J_5 \end{pmatrix} \quad (\text{根据引理 3})
\end{aligned}$$

其中 J_2,J_3,J_4,J_5 都是对角幂等矩阵, 而 A_2,A_3,A_4,A_5 都是可逆矩阵, 并且有性质

$$\det A_1(\det A_2)^{-1} \in S^*C/C, \qquad \det A_3 = \det A_2,$$

$$\det A \det A_3(\det A_4)^{-1} \in S^*C/C, \quad \det A_5 = \det A_4.$$

因此在映射 ψ 之下,

$$\begin{aligned}\Sigma\Sigma_1 \to \det A_5 S^*C/C =& \det A_4 S^*C/C = \det A \det A_3 S^*C/C \\ =& \det A \det A_2 S^*C/C = \det A S^*C/C \det A_1 S^*C/C.\end{aligned}$$

这就证明了定理 2.

§6 $U_n(K,H)$ 的换位子群 $(n=2\nu)$

在本节中我们仍假定 $n=2\nu$, 并采用 §5 节的记号, 首先我们证明

定理 1 $U_n'(K,H)$ 包有 $U_n(K,H)$ 的换位子群. 而且 $U_n'(K,H)$ 即是 $U_n(K,H)$ 的换位子群, 除开 $n=2$ 而且 $S=F_2$ 或 F_3 的情形和 $n=4$ 而且 $K=F_2$ 的情形.

【证】 本定理的第一个断言是定理 5.2 的直接推论, 因为 K^*/C 是交换群, 它的商群也是交换群.

要证本定理的第二个断言, 只要证明 $U_n'(K,H)$ 中任一元素皆可表成 $U_n(K,H)$ 中元素的换位子之积即可. 先以 $\mathfrak{C}$ 表 $U_n(K,H)$ 的换位子群. 证明分以下几步进行.

(i) 首先, 我们设 $n=2, \nu=1$, 而来证明一切

$$\begin{pmatrix} 1 & \lambda \\ 0 & 1 \end{pmatrix} \quad (\bar{\lambda}=\lambda)$$

皆属于 $\mathfrak{C}$. 如果 K 的特征数 $\neq 2,3$, 则对任意 $\bar{\lambda}=\lambda$,

$$\begin{pmatrix} 1 & 3\lambda \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} 2 & 0 \\ 0 & 2^{-1} \end{pmatrix}\begin{pmatrix} 1 & \lambda \\ 0 & 1 \end{pmatrix}\begin{pmatrix} 2 & 0 \\ 0 & 2^{-1} \end{pmatrix}^{-1}\begin{pmatrix} 1 & \lambda \\ 0 & 1 \end{pmatrix}^{-1},$$

$$\begin{pmatrix} 1 & 8\lambda \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} 3 & 0 \\ 0 & 3^{-1} \end{pmatrix}\begin{pmatrix} 1 & \lambda \\ 0 & 1 \end{pmatrix}\begin{pmatrix} 3 & 0 \\ 0 & 3^{-1} \end{pmatrix}^{-1}\begin{pmatrix} 1 & \lambda \\ 0 & 1 \end{pmatrix}^{-1},$$

都属于 $\mathfrak{C}$, 因此

$$\begin{pmatrix} 1 & \lambda \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} 1 & 3\lambda \\ 0 & 1 \end{pmatrix}^3\begin{pmatrix} 1 & 8\lambda \\ 0 & 1 \end{pmatrix}^{-1} \in \mathfrak{C},$$

我们的断言成立.

如果 K 的特征数 $=3$, 这时因 $S \neq F_3$, 故有 $\bar{\lambda}_1=\lambda_1 \neq 0, \pm 1$. 于是

$$\begin{pmatrix} 1 & \lambda_1^3-\lambda_1 \\ & 1 \end{pmatrix} = \begin{pmatrix} \lambda_1 & \\ & \lambda_1^{-1} \end{pmatrix}\begin{pmatrix} 1 & \lambda_1 \\ & 1 \end{pmatrix}\begin{pmatrix} \lambda_1 & \\ & \lambda_1^{-1} \end{pmatrix}^{-1}\begin{pmatrix} 1 & \lambda_1 \\ & 1 \end{pmatrix}^{-1} \in \mathfrak{C}.$$

因 $\lambda_1\neq 0,\pm 1$, 故 $\lambda_1^3-\lambda_1\neq 0$. 令 $\lambda_2=\lambda_1^3-\lambda_1$, 则 $\bar{\lambda}_2=\lambda_2\neq 0$ 而

$$\begin{pmatrix}1&\lambda_2\\0&1\end{pmatrix}\in\mathfrak{C}.$$

如 $\lambda_2=1$, 则

$$\begin{pmatrix}1&1\\0&1\end{pmatrix}\in\mathfrak{C};$$

如 $\lambda_2=-1$, 则

$$\begin{pmatrix}1&-1\\&1\end{pmatrix}^2\begin{pmatrix}0&1\\0&1\end{pmatrix}\in\mathfrak{C};$$

如 $\lambda_2\neq 0,\pm 1$, 则

$$\begin{pmatrix}\lambda_2^{-1}&\\&\lambda_2\end{pmatrix}\begin{pmatrix}1&\lambda_2\\&1\end{pmatrix}\begin{pmatrix}\lambda_2^{-1}&\\&\lambda_2\end{pmatrix}^{-1}=\begin{pmatrix}1&\lambda_2^{-1}\\&1\end{pmatrix}\in\mathfrak{C},$$

$$\begin{pmatrix}\lambda_2^{-1}+1&\\&(\lambda_2^{-1}+1)^{-1}\end{pmatrix}\begin{pmatrix}1&\lambda_2\\&1\end{pmatrix}$$

$$\begin{pmatrix}\lambda_2^{-1}+1&\\&(\lambda_2^{-1}+1)^{-1}\end{pmatrix}^{-1}=\begin{pmatrix}1&\lambda_2+\lambda_2^{-1}-1\\&1\end{pmatrix}\in\mathfrak{C},$$

于是也有

$$\begin{pmatrix}1&1\\&1\end{pmatrix}=\begin{pmatrix}1&\lambda_2+\lambda_2^{-1}-1\\&1\end{pmatrix}^{-1}\begin{pmatrix}1&\lambda_2\\&1\end{pmatrix}\begin{pmatrix}1&\lambda_2^{-1}\\&1\end{pmatrix}\in\mathfrak{C}.$$

我们证明了 $\mathfrak{C}$ 总包有 $\begin{pmatrix}1&1\\0&1\end{pmatrix}$. 于是 $\mathfrak{C}$ 包有

$$\begin{pmatrix}\lambda&\\&\lambda^{-1}\end{pmatrix}\begin{pmatrix}1&1\\&1\end{pmatrix}\begin{pmatrix}\lambda&\\&\lambda^{-1}\end{pmatrix}^{-1}=\begin{pmatrix}1&\lambda^2\\&1\end{pmatrix},$$

对一切 $\bar{\lambda}=\lambda\neq 0$, 因而包有

$$\begin{pmatrix}1&2\lambda\\&1\end{pmatrix}=\begin{pmatrix}1&(\lambda+1)^2\\&1\end{pmatrix}\begin{pmatrix}1&\lambda^2\\&1\end{pmatrix}^{-1}\begin{pmatrix}1&1\\&1\end{pmatrix}^{-1},$$

对一切 $\bar{\lambda} = \lambda \neq 0, -1$. 当 $\lambda = -1$ 时, $\begin{pmatrix} 1 & 2\lambda \\ & 1 \end{pmatrix} = \begin{pmatrix} 1 & 1 \\ & 1 \end{pmatrix}$ 已经属于 $\mathfrak{C}$. 故 $\mathfrak{C}$ 包有一切

$$\begin{pmatrix} 1 & 2\lambda \\ 0 & 1 \end{pmatrix} \quad (\bar{\lambda} = \lambda).$$

因此 $\mathfrak{C}$ 包有一切

$$\begin{pmatrix} 1 & \lambda \\ 0 & 1 \end{pmatrix} \quad (\bar{\lambda} = \lambda).$$

再研究 K 的特征数 $= 2$ 的情形. 如 $\lambda = \bar{\lambda} \neq 0, 1$, 则

$$\begin{pmatrix} 1 & \lambda^3 + \lambda^2 \\ & 1 \end{pmatrix} = \begin{pmatrix} \lambda + 1 & \\ & (\lambda+1)^{-1} \end{pmatrix} \begin{pmatrix} 1 & \lambda + 1 \\ & 1 \end{pmatrix}$$

$$\cdot \begin{pmatrix} \lambda + 1 & \\ & (\lambda+1)^{-1} \end{pmatrix}^{-1} \begin{pmatrix} 1 & \lambda + 1 \\ & 1 \end{pmatrix}^{-1} \in \mathfrak{C}.$$

因之

$$\begin{pmatrix} \lambda & \\ & \lambda^{-1} \end{pmatrix}^{-1} \begin{pmatrix} 1 & \lambda^3 + \lambda^2 \\ & 1 \end{pmatrix} \begin{pmatrix} \lambda & \\ & \lambda^{-1} \end{pmatrix} = \begin{pmatrix} 1 & \lambda + 1 \\ & 1 \end{pmatrix} \in \mathfrak{C},$$

对一切 $\lambda = \bar{\lambda} \neq 0, 1$; 即

$$\begin{pmatrix} 1 & \lambda \\ 0 & 1 \end{pmatrix} \in \mathfrak{C},$$

对一切 $\lambda = \bar{\lambda} \neq 0, 1$. 但是 $S \neq F_2$, 确有 $\lambda = \bar{\lambda} \neq 0, 1$, 故

$$\begin{pmatrix} 1 & 1 \\ & 1 \end{pmatrix} = \begin{pmatrix} 1 & \lambda + 1 \\ & 1 \end{pmatrix} \begin{pmatrix} 1 & \lambda \\ & 1 \end{pmatrix} \in \mathfrak{C},$$

所以这时我们的断言也成立.

(ii) 其次, 我们断言, 如 $n = 2\nu \geqslant 4$, 则

$$\begin{pmatrix} I^{(\nu)} & [0, \cdots, 0, \lambda, 0, \cdots, 0] \\ & I^{(\nu)} \end{pmatrix} \in \mathfrak{C},$$

对一切 $\bar{\lambda} = \lambda \neq 0$. 这只要证明当 $S = F_2$ 或 F_3 时, 我们的断言成立即可. 为书写方便起见, 设 $n = 4$. 注意

$$(1) \begin{pmatrix} A & \\ & \bar{A}'^{-1} \end{pmatrix} \begin{pmatrix} I & [\lambda, 0] \\ & I \end{pmatrix} \begin{pmatrix} A & \\ & \bar{A}'^{-1} \end{pmatrix}^{-1} \begin{pmatrix} I & [\lambda, 0] \\ & I \end{pmatrix}^{-1} = \begin{pmatrix} I & A \begin{pmatrix} \lambda & \\ & 0 \end{pmatrix} \bar{A}' - \begin{pmatrix} \lambda & \\ & 0 \end{pmatrix} \\ & I \end{pmatrix}$$

属于 $\mathfrak{C}$, 对一切 $\bar{\lambda}=\lambda\neq 0$ 及 $A\in SL_2(K)$. 先设 $S=F_3$, 这时 K 的特征数为 3. 取 $A=\begin{pmatrix} 1 & 0\\ \pm1 & 1\end{pmatrix}$, 则

$$\begin{pmatrix} 1 & 0\\ \pm1 & 1\end{pmatrix}\begin{pmatrix} \lambda & \\ & 0\end{pmatrix}\begin{pmatrix} 1 & \pm1\\ & 1\end{pmatrix}-\begin{pmatrix} \lambda & \\ & 0\end{pmatrix}=\begin{pmatrix} 0 & \pm\lambda\\ \pm\lambda & \lambda\end{pmatrix}.$$

因之 $\mathfrak{C}$ 包有

$$\begin{pmatrix} I & \begin{matrix} 0 & \lambda\\ \lambda & \lambda\end{matrix}\\ & I\end{pmatrix} \quad 和 \quad \begin{pmatrix} I & \begin{matrix} 0 & -\lambda\\ -\lambda & \lambda\end{matrix}\\ & I\end{pmatrix}.$$

所以 $\mathfrak{C}$ 包有它们的积

$$\begin{pmatrix} I & \begin{matrix} 0 & \lambda\\ \lambda & \lambda\end{matrix}\\ & I\end{pmatrix}\begin{pmatrix} I & \begin{matrix} 0 & -\lambda\\ -\lambda & \lambda\end{matrix}\\ & I\end{pmatrix}=\begin{pmatrix} I & \begin{matrix} 0 & 0\\ 0 & 2\lambda\end{matrix}\\ & I\end{pmatrix},$$

对一切 $\bar{\lambda}=\lambda\neq 0$. 于是 $\mathfrak{C}$ 包有

$$\begin{pmatrix} I & \begin{matrix} 0 & 0\\ 0 & \lambda\end{matrix}\\ & I\end{pmatrix},$$

对一切 $\bar{\lambda}=\lambda\neq 0$. 同理可证 $\mathfrak{C}$ 包有

$$\begin{pmatrix} I & \begin{matrix} \lambda & 0\\ 0 & 0\end{matrix}\\ & I\end{pmatrix},$$

对一切 $\bar{\lambda}=\lambda\neq 0$.

再设 $S=F_2$, 这时 K 的特征数 =2. 在 (1) 中取 $A=\begin{pmatrix} 1 & \\ 1 & 1\end{pmatrix}$, 则

$$\begin{pmatrix} 1 & \\ 1 & 1\end{pmatrix}\begin{pmatrix} \lambda & \\ & 0\end{pmatrix}\begin{pmatrix} 1 & 1\\ & 1\end{pmatrix}-\begin{pmatrix} \lambda & \\ & 0\end{pmatrix}=\begin{pmatrix} 0 & \lambda\\ \lambda & \lambda\end{pmatrix}.$$

如 $n\geqslant 6$, 为书写方便起见设 $n=6$. 则 $\mathfrak{C}$ 包有

$$\begin{pmatrix} I^{(3)} & \begin{matrix} 0 & \lambda & \\ \lambda & \lambda & \\ & & 0\end{matrix}\\ & I^{(3)}\end{pmatrix}.$$

同理 $\mathfrak{C}$ 也包有

$$\begin{pmatrix} I^{(3)} & \begin{matrix} \lambda & 0 & \lambda \\ 0 & 0 & 0 \\ \lambda & 0 & 0 \end{matrix} \\ & I^{(3)} \end{pmatrix} \text{ 及 } \begin{pmatrix} I^{(3)} & \begin{matrix} 0 & 0 & 0 \\ 0 & 0 & \lambda \\ 0 & \lambda & \lambda \end{matrix} \\ & I^{(3)} \end{pmatrix}.$$

于是 $\mathfrak{C}$ 包有

$$\begin{pmatrix} I^{(3)} & \begin{matrix} \lambda & \lambda & \lambda \\ \lambda & \lambda & \\ \lambda & & \end{matrix} \\ & I^{(3)} \end{pmatrix} = \begin{pmatrix} I^{(3)} & \begin{matrix} 0 & \lambda & \\ \lambda & \lambda & \\ & & 0 \end{matrix} \\ & I^{(3)} \end{pmatrix} \begin{pmatrix} I^{(3)} & \begin{matrix} \lambda & 0 & \lambda \\ 0 & 0 & 0 \\ \lambda & 0 & 0 \end{matrix} \\ & I^{(3)} \end{pmatrix}$$

以及

$$\begin{pmatrix} \begin{pmatrix} 1 & & \\ 1 & 1 & \\ 1 & & 1 \end{pmatrix} & \\ & \begin{pmatrix} 1 & & \\ 1 & 1 & \\ 1 & & 1 \end{pmatrix}'^{-1} \end{pmatrix} \begin{pmatrix} I^{(3)} & \begin{matrix} \lambda & \lambda & \lambda \\ \lambda & \lambda & \\ \lambda & & \end{matrix} \\ & I^{(3)} \end{pmatrix}$$

$$\cdot \begin{pmatrix} \begin{pmatrix} 1 & & \\ 1 & 1 & \\ 1 & & 1 \end{pmatrix} & \\ & \begin{pmatrix} 1 & & \\ 1 & 1 & \\ 1 & & 1 \end{pmatrix}'^{-1} \end{pmatrix}^{-1} = \begin{pmatrix} I^{(3)} & \begin{matrix} \lambda & & \\ & 0 & \lambda \\ & \lambda & \lambda \end{matrix} \\ & I^{(3)} \end{pmatrix}.$$

所以 $\mathfrak{C}$ 包有

$$\begin{pmatrix} I^{(3)} & \begin{matrix} \lambda & & \\ & 0 & \lambda \\ & \lambda & \lambda \end{matrix} \\ & I^{(3)} \end{pmatrix} \begin{pmatrix} I^{(3)} & \begin{matrix} 0 & & \\ & 0 & \lambda \\ & \lambda & \lambda \end{matrix} \\ & I^{(3)} \end{pmatrix} = \begin{pmatrix} I^{(3)} & \begin{matrix} \lambda & & \\ & 0 & \\ & & 0 \end{matrix} \\ & I^{(3)} \end{pmatrix},$$

对一切 $\bar{\lambda}=\lambda\neq 0$. 即我们的断言成立. 如果 $n=4$, 则 $K=F_4$. 令 $F_4=F_2(x), x^2+x+1=0$. 在 (1) 中取 $A=\begin{pmatrix}1 & \\ 1 & 1\end{pmatrix}$, 注意这时 $\lambda=1$, 故

$$\begin{pmatrix}1 & \\ 1 & 1\end{pmatrix}\begin{pmatrix}\lambda & \\ & 0\end{pmatrix}\begin{pmatrix}1 & 1\\ & 1\end{pmatrix}-\begin{pmatrix}\lambda & \\ & 0\end{pmatrix}=\begin{pmatrix}0 & \lambda\\ \lambda & \lambda\end{pmatrix}=\begin{pmatrix}0 & 1\\ 1 & 1\end{pmatrix}.$$

再在 (1) 中取 $A=\begin{pmatrix}1 & \\ x & 1\end{pmatrix}$, 则

$$\begin{pmatrix}1 & \\ x & 1\end{pmatrix}\begin{pmatrix}\lambda & \\ & 0\end{pmatrix}\begin{pmatrix}1 & \bar{x}\\ & 1\end{pmatrix}-\begin{pmatrix}\lambda & \\ & 0\end{pmatrix}=\begin{pmatrix} & \bar{x}\\ x & 1\end{pmatrix}.$$

于是 $\mathfrak{C}$ 包有

$$\begin{pmatrix}I & 0 & 1 & \\ & 1 & 1 & \\ & & & I\end{pmatrix} \text{ 及 } \begin{pmatrix}I & 0 & \bar{x} & \\ & x & 1 & \\ & & & I\end{pmatrix}.$$

因而 $\mathfrak{C}$ 包有

$$\begin{pmatrix}I & 0 & x & \\ & \bar{x} & 0 & \\ & & & I\end{pmatrix}=\begin{pmatrix}I & 0 & 1 & \\ & 1 & 1 & \\ & & & I\end{pmatrix}\begin{pmatrix}I & 0 & \bar{x} & \\ & x & 1 & \\ & & & I\end{pmatrix}$$

以及

$$\begin{pmatrix}\begin{pmatrix}1 & 1\\ & 1\end{pmatrix} & \\ & \begin{pmatrix}1 & 1\\ & 1\end{pmatrix}^{\prime -1}\end{pmatrix}\begin{pmatrix}I & 0 & x & \\ & \bar{x} & 0 & \\ & & & I\end{pmatrix}$$

$$\cdot\begin{pmatrix}\begin{pmatrix}1 & 1\\ & 1\end{pmatrix} & \\ & \begin{pmatrix}1 & 1\\ & 1\end{pmatrix}^{\prime -1}\end{pmatrix}^{-1}=\begin{pmatrix}I & 1 & x & \\ & \bar{x} & 0 & \\ & & & I\end{pmatrix},$$

所以 $\mathfrak{C}$ 包有

$$\begin{pmatrix}I & 0 & x & \\ & \bar{x} & 0 & \\ & & & I\end{pmatrix}\begin{pmatrix}I & 1 & x & \\ & \bar{x} & 0 & \\ & & & I\end{pmatrix}=\begin{pmatrix}I & 1 & 0 & \\ & 0 & 0 & \\ & & & I\end{pmatrix}.$$

故这时我们的断言 (ii) 也成立.

(iii) 现在我们证明 $\mathfrak{C}$ 包有一切

$$\begin{pmatrix} I & Y \\ & I \end{pmatrix} \quad (\bar{Y}' = Y).$$

如 Y 不是交错矩阵, 则有 $\nu \times \nu$ 可逆矩阵 P 存在, 使

$$PY\bar{P}' = [\lambda_1, \cdots, \lambda_r, 0, \cdots, 0] \quad (\overline{\lambda_i} = \lambda_i; 1 \leqslant i \leqslant r).$$

于是

$$\begin{aligned}\begin{pmatrix} I & Y \\ & I \end{pmatrix} &= \begin{pmatrix} P^{-1} & \\ & \bar{P}' \end{pmatrix}\begin{pmatrix} I & [\lambda_1, \cdots, \lambda_r, 0, \cdots, 0] \\ & I \end{pmatrix}\begin{pmatrix} P^{-1} & \\ & \bar{P}' \end{pmatrix}^{-1} \\ &= \begin{pmatrix} P^{-1} & \\ & \bar{P}' \end{pmatrix}\begin{pmatrix} I & [\lambda_1, 0, \cdots, 0] \\ & I \end{pmatrix}\begin{pmatrix} P^{-1} & \\ & \bar{P}' \end{pmatrix}^{-1} \cdots \\ &\quad \cdot \begin{pmatrix} P^{-1} & \\ & \bar{P}' \end{pmatrix}\begin{pmatrix} I & [0, \cdots, 0, \lambda_r, 0, \cdots, 0] \\ & I \end{pmatrix}\begin{pmatrix} P^{-1} & \\ & \bar{P}' \end{pmatrix}^{-1}\end{aligned}$$

属于 $\mathfrak{C}$. 如 Y 交错, 这时 K 是特征数为 2 的域而 $a \to \bar{a}$ 是单位自同构. 于是 $Y + [1, 0, \cdots, 0]$ 不交错. 因此

$$\begin{pmatrix} I & Y \\ & I \end{pmatrix} = \begin{pmatrix} I & Y + [1, 0, \cdots, 0] \\ & I \end{pmatrix}\begin{pmatrix} I & [1, 0, \cdots, 0] \\ & I \end{pmatrix} \in \mathfrak{C}.$$

同理可证 $\mathfrak{C}$ 包有一切

$$\begin{pmatrix} I & \\ X & I \end{pmatrix} \quad (\bar{X}' = X).$$

(iv) 像定理 2.1 的证明中一样, 可以推出

$$\begin{pmatrix} I - J & J \\ -J & I - J \end{pmatrix} \in \mathfrak{C},$$

对一切对角形矩阵 $J = J^2$; 以及

$$\begin{pmatrix} A & 0 \\ 0 & \bar{A}'^{-1} \end{pmatrix} \in \mathfrak{C},$$

对一切 $A \in SL_\nu(K)$; 以及

(2) $$\begin{pmatrix} D(\lambda) & 0 \\ 0 & \overline{D(\lambda)}'^{-1} \end{pmatrix} \in \mathfrak{C}$$

对一切 $D(\lambda)=[1,\cdots,1,\lambda], \bar{\lambda}=\lambda$. 由于

(3) $$\begin{pmatrix} a & \\ & \bar{a}^{-1} \end{pmatrix}\begin{pmatrix} b & \\ & \bar{b}^{-1} \end{pmatrix}\begin{pmatrix} a^{-1} & \\ & \bar{a} \end{pmatrix}\begin{pmatrix} b^{-1} & \\ & \bar{b} \end{pmatrix}=\begin{pmatrix} aba^{-1}b^{-1} & \\ & \overline{(aba^{-1}b^{-1})}^{-1} \end{pmatrix}\in \mathfrak{C},$$

所以

$$\begin{pmatrix} c & \\ & \bar{c}^{-1} \end{pmatrix} \in \mathfrak{C},$$

对一切 $c \in C$.

(v) 最后, 设 $\Sigma \in U_n'(K,H)$. 将 Σ 表成形状

$$\Sigma = \begin{pmatrix} A & B \\ C & D \end{pmatrix}\begin{pmatrix} I-J & J \\ -J & I-J \end{pmatrix},$$

其中 A 可逆而 $J^2=J$ 为对角形矩阵. 因 $\Sigma \in U_n'(K,H)$, 故

$$\det A \in S^*C/C.$$

将 Σ 表作

$$\Sigma = \begin{pmatrix} A & \\ & \bar{A}'^{-1} \end{pmatrix}\begin{pmatrix} I & \\ X & I \end{pmatrix}\begin{pmatrix} I & Y \\ & I \end{pmatrix}\begin{pmatrix} I-J & J \\ -J & I-J \end{pmatrix},$$

再将 A 表作

$$A = D(\mu)B,$$

其中 $D(\mu)=[1,\cdots,1,\mu], B \in SL_\nu(K)$. 要证明 $\Sigma \in \mathfrak{C}$, 只要证明

(4) $$\begin{pmatrix} D(\mu) & 0 \\ & \overline{D(\mu)}^{-1} \end{pmatrix} \in \mathfrak{C}.$$

因为 $\det A = \mu C$, 而

$$\det A \in S^*C/C,$$

所以

$$\mu C \in S^*C/C.$$

因此 $\mu \in S^*C$, 这样, 从 (2), (3) 即可推出 (4).

定理 1 至此完全证明了.

最后我们研究 $U_n'(K,H)$ 与 $TU_n(K,H)$ 的关系.

定理 2 设 $n=2\nu$, 则 $TU_n(K,H) \subset U_n'(K,H)$.

【证】 设 T 是一个酉平延, 则有 $U \in U_n(K,H)$, 使

$$T_1 = UTU^{-1} = \begin{pmatrix} I & [\lambda, 0, \cdots, 0] \\ & I \end{pmatrix} \quad (\bar{\lambda} = \lambda \neq 0).$$

显然 $T_1 \in U_n'(K,H)$. 因 $U_n'(K,H)$ 是 $U_n(K,H)$ 的正规子群, 故 $T \in U_n'(K,H)$. 因此 $TU_n(K,H) \subset U_n'(K,H)$.

定理 3　设 $n = 2\nu > 2$, 则 $TU_n(K,H) = U_n'(K,H)$.

【证】 只需证 $U_n'(K,H) \subset TU_n(K,H)$. 根据 $U_n'(K,H)$ 的定义及定理 2.1 的证明, 这是很显然的.

注意, 当 $n = 2\nu = 2$ 时, 有例表明 $U_2'(K,H) \neq TU_2(K,H)$. 设 K 是特征数 $\neq 2$ 的域 Z 上的广义四元数体, 则

$$TU_2(K,H) = TU_2(Z,H) = SL_2(Z,H).$$

但是元素

$$\begin{pmatrix} \alpha & \\ & \bar{\alpha}^{-1} \end{pmatrix} \in U_2'(K,H),$$

如果 $\alpha\bar{\alpha} = 1$, 即 α 的范数是 1.

定理 4　设 $n = 2\nu > 2$, 则

$$U_n(K,H)/TU_n(K,H) \approx (K^*/C)/(S^*C/C) \approx K^*/S^*C.$$

更进一步, $TU_n(K,H)$ 还是 $U_n(K,H)$ 的换位子群, 除开 $n = 4$ 而 $K = F_2$ 这一情形.

第九章　特征数 $\neq 2$ 的域上的正交群的构造 $(\nu \geqslant 1)$

§1　复　　习

前面已经提到过, 如果我们把特征数 $\neq 2$ 的域 F 的单位自同构看作是它的对合性反自同构, 那么就可以把 F 上的对称矩阵看作是哈矩阵, 因此还可以把 F 上对于非退化对称矩阵 S 的正交群看作是对哈矩阵 S 的酉群. 因此第七章中关于酉群的一些结果对于正交群也成立, 但应注意的是正交群里没有平延.

为了今后的需要, 我们把所需要的第七章中的结果重新叙述如下:

定理 1　设 X 和 Y 是两个 p 秩的 $p\times n$ 矩阵. 那么, $O_n(F,S)$ 里有一个元素 T 存在, 使 $X=YT$ 的必要且充分条件是 $XSX'=YSY'$.

这是第七章定理 6.1 的系理 2.

当 $\nu=\dfrac{n}{2}$ 时, 不失去普遍性, 我们可以假定

$$S=\begin{pmatrix} 0 & I^{(\nu)} \\ I^{(\nu)} & 0 \end{pmatrix}.$$

于是第七章 §7 的主要结果可以归纳成

定理 2　当 $\nu=\dfrac{n}{2}$ 时, 以下这些元素都是 $O_n(F,S)$ 里的元素:

(1) $\begin{pmatrix} A & \\ & A'^{-1} \end{pmatrix}$　(A 是 ν 行 ν 列的可逆矩阵);

(2) $\begin{pmatrix} I & Q \\ & I \end{pmatrix}$ 及 $\begin{pmatrix} I & \\ Q & I \end{pmatrix}$　(Q 是斜对称矩阵, 即 $Q'=-Q$);

(3) $\begin{pmatrix} J & I-J \\ I-J & J \end{pmatrix}$　($J^2=J$ 是对角矩阵);

而且, $O_n(F,S)$ 里每一个元素, 都可以表成下面的形状;

(4) $\begin{pmatrix} I & \\ X & I \end{pmatrix}\begin{pmatrix} A & \\ & A'^{-1} \end{pmatrix}\begin{pmatrix} I & Y \\ & I \end{pmatrix}\begin{pmatrix} J & I-J \\ I-J & J \end{pmatrix}$,

这里 $X'=-X, Y'=-Y, A$ 是可逆的, 而 $J^2=J$ 是对角矩阵.

当 $0<2\nu<n$ 时, 不失去普遍性, 我们可以假定

$$S=\begin{pmatrix} 0 & I^{(\nu)} & \\ I^{(\nu)} & 0 & \\ & & \Delta \end{pmatrix},$$

而 $\Delta=\Delta^{(n-2\nu)}$ 是定号的对角形矩阵. 于是第七章 §8 节的主要结果可以归纳成

定理 3 当 $0<2\nu<n$ 时, 以下这些元素都是 $O_n(F,S)$ 里的元素:

(5) $\begin{pmatrix} A & B & \\ C & D & \\ & & I \end{pmatrix}$, 而 $\begin{pmatrix} A & B \\ C & D \end{pmatrix}$ 在 $O_{2\nu}(F,S_1)$ 中, $S_1=\begin{pmatrix} 0 & I^{(\nu)} \\ I^{(\nu)} & 0 \end{pmatrix}$;

(6) $\begin{pmatrix} I & & \\ & I & \\ & & U \end{pmatrix}$, 而 U 在 $O_{n-2\nu}(F,\Delta)$ 中;

(7) $\begin{pmatrix} J & I-J & \\ I-J & J & \\ & & I \end{pmatrix}$, 而 $J^2=J$ 是对角矩阵;

(8) $\begin{pmatrix} I^{(\nu)} & -\frac{1}{2}P\Delta P' & -P \\ & I^{(\nu)} & \\ & \Delta P' & I^{(n-2\nu)} \end{pmatrix}$ 和 $\begin{pmatrix} I & & \\ -\frac{1}{2}P\Delta P' & I & -P \\ \Delta P' & & I \end{pmatrix}$,

而 $P=P^{(\nu,n-2\nu)}$ 是任意的; 而且, $O_n(F,S)$ 里每一个元素都可以表成下面的形状:

(9) $\begin{pmatrix} I & & \\ -\frac{1}{2}X\Delta X' & I & -X \\ \Delta X' & & I \end{pmatrix}\begin{pmatrix} A & B & \\ C & D & \\ & & U \end{pmatrix}\begin{pmatrix} I & -\frac{1}{2}Y\Delta Y' & -Y \\ & I & \\ & \Delta Y' & I \end{pmatrix}\begin{pmatrix} J & I-J & \\ I-J & J & \\ & & I \end{pmatrix}$.

定义 正交群里的一个元素 T 称为对称, 如果 $T^2=I$ 而且 $T-I$ 是秩为 1 的.

定理 4 设 T 是正交群里的对称, 那么适合 $vT=-v$ 的向量组成一个一维的非迷向向量空间 V, 称为 T 的负空间, 而 V^* 则是所有适合 $vT=v$ 的向量的全体. 反之, 给了一个任意一维的非迷向向量空间就有一个唯一的对称以这个空间为负空间. 更进一步, 以非迷向向量 v 所生成的空间为负空间的对称 T 可以表成下面的形状:

(10) $$T=I-2Sv'(vSv')^{-1}v.$$

这个定理是第七章定理 9.2 的特殊情形.

我们要用到下面这个基本的定理:

定理 5　$O_n(F,S)$ 是由对称所演成的. 更进一步, $O_n(F,S)$ 里每个元素都可以用不多于 n 个对称的乘积表出来.

先证以下几个引理.

引理 1　设 A 为一个 $n\times n$ 对称矩阵, 若 $xSx'\neq 0$ 的 n 维向量 x 皆使 $xAx'=0$, 则 $A=0$, 除非 $n=2, F=F_3$ 而 S 合同于 $\pm\begin{pmatrix}1 & 0\\ 0 & -1\end{pmatrix}$.

【证】　不妨设 S 为对角形矩阵

$$S=\begin{pmatrix}s_1 & & & 0\\ & s_2 & & \\ & & \ddots & \\ 0 & & & s_n\end{pmatrix}.$$

写

$$A=\begin{pmatrix}a_{11} & a_{12} & \cdots & a_{1n}\\ a_{21} & a_{22} & \cdots & a_{2n}\\ \cdots & \cdots & \cdots & \cdots\\ a_{n1} & a_{n2} & \cdots & a_{nn}\end{pmatrix}.$$

取 $e_1=(1,0,\cdots,0)$, 则 $e_1Se_1'\neq 0$. 于是从 $e_1Ae_1'=0$ 推出 $a_{11}=0$. 同理 $a_{22}=\cdots=a_{nn}=0$.

取 $e_{12}=(1,1,0,\cdots,0)$. 如 $e_{12}Se_{12}'\neq 0$, 则从 $e_{12}Ae_{12}'=0$ 推出 $a_{12}=0$. 如 $e_{12}Se_{12}'=0$ 而 $n\geqslant 3$, 令 $e_n=(0,0,\cdots,0,1)$, 则 $(e_{12}\pm e_n)S(e_{12}\pm e_n)'\neq 0$, 于是从 $(e_{12}\pm e_n)A(e_{12}\pm e_n)'=0$ 也推出 $a_{12}=0$. 因此, 如 $n\geqslant 3$, 同理可证 $a_{ij}=0\ (i<j)$, 于是 $A=0$.

最后考查 $n=2$ 的情形. 这时

$$S=\begin{pmatrix}s_1 & 0\\ 0 & s_2\end{pmatrix}.$$

如 $s_1\neq -s_2$, 亦有 $e_{12}Se_{12}'\neq 0$, 因此这时也有 $A=0$. 如 $s_1=-s_2$, 写

$$S=\begin{pmatrix}s & 0\\ 0 & -s\end{pmatrix}.$$

如 $F\neq F_3$, 则有 $\lambda\in F^*$, 使 $1-\lambda^2\neq 0$. 于是

$$(1,\lambda)S(1,\lambda)'=(1-\lambda^2)s\neq 0,$$

因此从 $(1,\lambda)A(1,\lambda)'=0$ 也推出 $a_{12}=0$. 因此也有 $A=0$.

这就证明了引理 1.

引理 2　设 x 和 y 是两个 n 维向量, 具性质:

$$xSx' = ySy' \text{ 及 } (x-y)S(x-y)' \neq 0,$$

则有一对称 W 存在, 使 $y = xW$.

【证】　因 $x-y$ 非迷向, 不妨设

$$x - y = (a, 0, \cdots, 0)$$

而

$$S = \begin{pmatrix} s & 0 \\ 0 & S_1^{(n-1)} \end{pmatrix}.$$

于是取

$$W = \begin{pmatrix} -1 & 0 \\ 0 & I^{(n-1)} \end{pmatrix},$$

则 $(x-y)W = -(x-y)$, 即

(11)

$$x(W+1) = y(W+I).$$

当

$$x = (x_1, \cdots, x_n), \quad y = (y_1, \cdots, y_n),$$

则从 (11) 式推出 $x_2 = y_2, \cdots, x_n = y_n$. 再从 $xSx' = ySy'$ 推出 $x_1^2 = y_1^2$. 因 $x \neq y$, 故 $x_1 = -y_1$. 因此 $y = xW$.

现在来证明定理 5. 先考查 $n = 2, F = F_3$ 及 $S = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$ 这个情形.

$O_2\left(F_3, \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}\right)$ 一共由四个元素, 即

$$\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} -1 & 0 \\ 0 & -1 \end{pmatrix}, \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}, \begin{pmatrix} -1 & 0 \\ 0 & 1 \end{pmatrix}$$

组成. 这时定理 5 显然成立. 在以下的讨论中, 我们永远除去这一特殊情形.

设 $T \in O_n(F, S)$. 我们用归纳法像 n 来证明 T 可表成不多于 n 个对称之积.

先设有一非迷向向量 x(即$xSx' \neq 0$) 存在, 使 $xT = x$. 这时, 可将 S 和 T 同时化为

$$S = \begin{pmatrix} s & 0 \\ 0 & S_1^{(n-1)} \end{pmatrix}, \quad T = \begin{pmatrix} 1 & 0 \\ 0 & T_1^{(n-1)} \end{pmatrix},$$

其中 S_1 是 $(n-1)\times(n-1)$ 对称矩阵而 $T_1\in O_{n-1}(F,S_1)$. 于是依归纳法假设, T_1 可表成不多于 $n-1$ 个对称之积, 因此 T 也可表成不多于 $n-1$ 个对称之积.

再研究

$$A=(T-I)S(T-I)'.$$

分以下两种情形来讨论:

(i) $A\neq 0$, 依引理 1, 有 n 维向量 x 存在, 使

$$xSx'\neq 0 \quad \text{及} \quad xAx'\neq 0.$$

令

$$y=xT.$$

于是

$$xSx'=ySy',$$

$$(x-y)S(x-y)'=x(I-T)S(I-T)'x'=xAx'\neq 0.$$

因此依引理 2, 有对称 W 存在, 使 $x=yW$. 于是

$$x=xTW.$$

根据适才证明的断言, TW 可表成不多于 $n-1$ 个对称之积, 因此 T 可表成不多于 n 个对称之积.

(ii) $A=0$. 即

$$(T-I)S(T-I)'=0,$$

也即

$$TS+ST'=2S.$$

将 T 左乘上式, 得

$$T^2S+S=2TS,$$

消去 S 得

$$(T-I)^2=0.$$

在相似变换之下 T 可化为

$$\begin{pmatrix} I^{(\nu)} & I^{(\nu)} & 0 \\ 0 & I^{\nu} & 0 \\ 0 & 0 & I^{(r)} \end{pmatrix} \quad (2\nu+r=n).$$

因此不妨设

$$T = \begin{pmatrix} I^{(\nu)} & I^{(\nu)} & 0 \\ 0 & I^{(\nu)} & 0 \\ 0 & 0 & I^{(r)} \end{pmatrix}.$$

若有一 n 维向量 x, 使 $xT = x$ 及 $xSx' \neq 0$, 前面已经证明 T 可表成不多于 $n-1$ 个对称之积, 于是问题已经解决, 因此唯一没有解决的情形是对一切 x 使 $xT = x$ 者, 恒有 $xSx' = 0$. 这时

$$S = \begin{pmatrix} S^{(\nu)} & * \\ * & 0^{(\nu+r)} \end{pmatrix}.$$

如 $r > 0$, 则 S 奇异, 此为不可能; 因此 $r = 0$, 于是一定有

$$T = \begin{pmatrix} I^{(\nu)} & I^{(\nu)} \\ 0 & I^{(\nu)} \end{pmatrix} \quad (n = 2\nu).$$

这时 $\det T = 1$. 设 W 为一对称, 则 $\det TW = -1$. 对 TW 重复上述对 T 的证明, 情形 (ii) 不能发生, 因此 TW 可表成不多于 n 个对称之积, 因此 T 可表成不多于 $n+1$ 个对称之积. 因 $n = 2\nu$ 是偶数, 而 $\det T = 1$, 所以 T 不能表成 $n+1$ 个对称之积, 因而 T 可表成不多于 n 个对称之积.

这样定理 5 就完全证明了.

最后, 以 $\Omega_n(F,S)$ 表 $O_n(F,S)$ 的换位子群. 于是, 我们有正规群列

$$O_n(F,S) \supset O_n^+(F,S) \supset \Omega_n(F,S) \supset \Omega_n(F,S) \cap Z_n \supset \{I\},$$

其中 Z_n 表 $GL_n(F)$ 的中心. 显然有

$$O_n(F,S) : O_n^+(F,S) = 2.$$

在本章以下诸节中, 我们将在 $\nu \geqslant 1$ 的假设下证明 $\Omega_n(F,S) \cap Z_n$ 即是 $\Omega_n(F,S)$ 的中心, 并研究商群

$$O_n^+(F,S)/\Omega_n(F,S) \quad 和 \quad \Omega_n(F,S)/\Omega_n(F,S) \cap Z_n$$

的构造. 我们将 $\Omega_n(F,S)/\Omega_n(F,S) \cap Z_n$ 记作 $P\Omega_n(F,S)$.

§2　由 2 平延所演成的群

在本节中我们总假定 $\nu \geqslant 2$.

定义 正交群中的元素 $T = I + N$ 称为 2 平延, 如果 N 的秩是 2, 而且 $NSN' = 0$.

从 $(I+N)S(I+N)' = S$ 我们可以推出 $NS + SN' = 0$. 因此 NS 是斜对称的. 于是我们可以把 NS 写成

$$NS = \begin{pmatrix} x_1 \\ x_2 \end{pmatrix}' \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix} \begin{pmatrix} x_1 \\ x_2 \end{pmatrix},$$

其中 x_1 和 x_2 都是 n 维向量. 那么

$$N = \begin{pmatrix} x_1 \\ x_2 \end{pmatrix}' \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix} \begin{pmatrix} x_1 \\ x_2 \end{pmatrix} S^{-1}.$$

令

$$\begin{pmatrix} v_1 \\ v_2 \end{pmatrix} = \begin{pmatrix} x_1 \\ x_2 \end{pmatrix} S^{-1},$$

我们就有

$$N = S \begin{pmatrix} v_1 \\ v_2 \end{pmatrix}' \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix} \begin{pmatrix} v_1 \\ v_2 \end{pmatrix}.$$

于是 2 平延 T 就可以表成

(1)
$$T = I + S \begin{pmatrix} v_1 \\ v_2 \end{pmatrix}' \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix} \begin{pmatrix} v_1 \\ v_2 \end{pmatrix}.$$

因为 $NSN' = 0$, 所以

$$\begin{pmatrix} v_1 \\ v_2 \end{pmatrix} S \begin{pmatrix} v_1 \\ v_2 \end{pmatrix}' = 0.$$

定理 1 在 $O_n(F, S)$ 之下, 任一 2 平延都相似于

(2)
$$\begin{pmatrix} I & K & \\ & I & \\ & & I \end{pmatrix}, \text{而} K = \begin{pmatrix} 0 & 1 & \\ -1 & 0 & \\ & & 0 \end{pmatrix};$$

也相似于

(3)
$$\begin{pmatrix} A & & \\ & A'^{-1} & \\ & & I \end{pmatrix}, \text{而} A = \begin{pmatrix} 1 & 1 & \\ & 1 & \\ & & I \end{pmatrix}.$$

【证】 设 T 是任一 2 平延, 那么我们可以把 T 表成 (1). 因为

$$\begin{pmatrix} 1 & 0 & 0 & \cdots & 0 \\ 0 & 1 & 0 & \cdots & 0 \end{pmatrix} S \begin{pmatrix} 1 & 0 & 0 & \cdots & 0 \\ 0 & 1 & 0 & \cdots & 0 \end{pmatrix}' = 0,$$

依定理 1.1, 就有一个正交矩阵 P 存在, 使

$$\begin{pmatrix} v_1 \\ v_2 \end{pmatrix} = \begin{pmatrix} 1 & 0 & 0 & \cdots & 0 \\ 0 & 1 & 0 & \cdots & 0 \end{pmatrix} P.$$

那么

$$PTP^{-1} = \begin{pmatrix} I & & \\ K & I & \\ & & I \end{pmatrix},$$

而

$$\begin{pmatrix} 0 & I & \\ I & 0 & \\ & & I \end{pmatrix} \begin{pmatrix} I & & \\ K & I & \\ & & I \end{pmatrix} \begin{pmatrix} 0 & I & \\ I & 0 & \\ & & I \end{pmatrix} = \begin{pmatrix} I & K & \\ & I & \\ & & I \end{pmatrix}.$$

同样, 我们也可以证明 T 相似于 (3).

今后, 我们用 $\mathfrak{T}$ 表示 $O_n(F,S)$ 中由 2 平延所演成的子群. 显然, $\mathfrak{T}$ 是 $O_n(F,S)$ 的正规子群.

定理 2　以下这些元素都是 $\mathfrak{T}$ 的元素:

(4) $\begin{pmatrix} I & K & \\ & I & \\ & & I \end{pmatrix}$ 及 $\begin{pmatrix} I & & \\ K & I & \\ & & I \end{pmatrix}$　($K' = -K$ 是任意斜对称矩阵);

(5) $\begin{pmatrix} A & & \\ & A'^{-1} & \\ & & I \end{pmatrix}$, 而 $\det A \in F^{*2}$;

(6) $\begin{pmatrix} I-J & J & \\ J & I-J & \\ & & I \end{pmatrix}$　($J^2 = J$ 是偶秩的对角矩阵);

(7) $\begin{pmatrix} I & -\frac{1}{2}P\Delta P' & -P \\ & I & \\ & \Delta P' & I \end{pmatrix}$ 和 $\begin{pmatrix} I & & \\ -\frac{1}{2}P\Delta P' & I & -P \\ \Delta P' & & I \end{pmatrix}$ (P是任意的ν行$n-2\nu$列矩阵).

【证】 因为 $\mathfrak{T}$ 包有 (2), 而

$$\begin{pmatrix} P & \\ & P'^{-1} \end{pmatrix}\begin{pmatrix} I & K \\ & I \end{pmatrix}\begin{pmatrix} P & \\ & P'^{-1} \end{pmatrix}^{-1} = \begin{pmatrix} I & PKP' \\ & I \end{pmatrix}$$

和

$$\begin{pmatrix} I & K_1 \\ & I \end{pmatrix}\begin{pmatrix} I & K_2 \\ & I \end{pmatrix} = \begin{pmatrix} I & K_1+K_2 \\ & I \end{pmatrix},$$

所以 $\mathfrak{T}$ 包有 (4).

因为 $\mathfrak{T}$ 包有 (3), 而 $SL_\nu(F)$ 是由 $\begin{pmatrix} 1 & 1 & \\ & 1 & \\ & & I \end{pmatrix}$ 和它在 $GL_\nu(F)$ 里的共轭元素所生成的, 所以 $\mathfrak{T}$ 包有 (5), 其中 $A \in SL_\nu(F)$. 设 $A \in GL_\nu(F)$, 而 $\det A = \lambda^2 (\lambda \neq 1)$. 由

$$\begin{pmatrix} I & K_1 \\ & I \end{pmatrix}\begin{pmatrix} I & \\ K_2 & I \end{pmatrix} = \begin{pmatrix} I+K_1K_2 & K_1 \\ K_2 & I \end{pmatrix} = \begin{pmatrix} I & \\ K_2(I+K_1K_2)^{-1} & I \end{pmatrix}$$

$$\cdot \begin{pmatrix} I+K_1K_2 & \\ & (I+K_1K_2)'^{-1} \end{pmatrix}\begin{pmatrix} I & (I+K_1K_2)^{-1}K_1 \\ & I \end{pmatrix},$$

其中 $K_1' = -K_1, K_2' = -K_2$, 而 $I+K_1K_2 \in GL_\nu(F)$, 我们取

$$K_1 = \begin{pmatrix} 0 & 1 & \\ -1 & 0 & \\ & & I \end{pmatrix}, \quad K_2 = \begin{pmatrix} 0 & 1-\lambda^{-1} & \\ -(1-\lambda^{-1}) & 0 & \\ & & I \end{pmatrix},$$

于是, $\mathfrak{T}$ 包有

$$\begin{pmatrix} A_1 & & \\ & A_1'^{-1} & \\ & & I \end{pmatrix}, \text{而} A_1 = \begin{pmatrix} \lambda^{-1} & & \\ & \lambda^{-1} & \\ & & I \end{pmatrix}.$$

再由 $\det(A_1A) = 1$, 就有 $\mathfrak{T}$ 包有

$$\begin{pmatrix} A_1A & & \\ & (A_1A)'^{-1} & \\ & & I \end{pmatrix} = \begin{pmatrix} A_1 & & \\ & A_1'^{-1} & \\ & & I \end{pmatrix}\begin{pmatrix} A_1 & & \\ & A'^{-1} & \\ & & I \end{pmatrix},$$

因而 $\mathfrak{T}$ 包有 (5).

从下面这个等式

$$\begin{pmatrix} I^{(2)} & K \\ & I^{(2)} \end{pmatrix} \begin{pmatrix} I & \\ K & I \end{pmatrix} \begin{pmatrix} I & K \\ & I \end{pmatrix} \begin{pmatrix} -K & \\ & -K \end{pmatrix} = \begin{pmatrix} 0 & I \\ I & 0 \end{pmatrix},$$

其中 $K = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}$, 我们就可以推出来 $\mathfrak{T}$ 包有 (6).

最后, 从

$$\begin{aligned} &\begin{pmatrix} A_1 & & \\ & A'^{-1} & \\ & & I \end{pmatrix}^{-1} \begin{pmatrix} I & -\frac{1}{2}P\Delta P' & -P \\ & I & \\ & \Delta P' & I \end{pmatrix} \cdot \\ &\cdot \begin{pmatrix} A_1 & & \\ & A'^{-1} & \\ & & I \end{pmatrix}^{-1} \begin{pmatrix} I & -\frac{1}{2}P\Delta P' & -P \\ & I & \\ & \Delta P' & I \end{pmatrix}^{-1} \\ = &\begin{pmatrix} I & -\frac{1}{2}(AP\Delta P' - P\Delta P'A') & \\ & I & \\ & & I \end{pmatrix} \cdot \\ &\cdot \begin{pmatrix} I & -\frac{1}{2}(P-AP)\Delta(P-AP)' & P-AP \\ & I & \\ & -\Delta(P-AP)' & I \end{pmatrix}, \end{aligned}$$

我们就推出来 $\mathfrak{T}$ 包有 (7), 而其中 P 取特殊形式 $P - AP$, 这里 $\det A \in F^{*2}$. 我们可以选取 A 和 P, 使 $P - AP$ 跑过所有只有一行不为 0 的矩阵. 又因为

$$\begin{aligned} &\begin{pmatrix} I & -\frac{1}{2}P\Delta P' & -P \\ & I & \\ & \Delta P' & I \end{pmatrix} \begin{pmatrix} I & -\frac{1}{2}Q\Delta Q' & -Q \\ & I & \\ & \Delta Q' & I \end{pmatrix} \\ = &\begin{pmatrix} I & -\frac{1}{2}(P\Delta Q' - Q\Delta P') & \\ & I & \\ & & I \end{pmatrix} \begin{pmatrix} I & -\frac{1}{2}(P+Q)\Delta(P+Q)' & -(P+Q) \\ & I & \\ & \Delta(P+Q)' & I \end{pmatrix}, \end{aligned}$$

所以 $\mathfrak{T}$ 包有所有形如 (7) 的矩阵. 定理完全证明.

定理 3 给了任意一个 $U \in O_{n-2\nu}(F, \Delta)$, F 里就有一个元素 $a \neq 0$ 存在, 使

$$\begin{pmatrix} a & & & & \\ & I & & & \\ & & a^{-1} & & \\ & & & I & \\ & & & & U \end{pmatrix} \text{ 或 } \begin{pmatrix} 0 & & a & & \\ & I & & & \\ a^{-1} & & 0 & & \\ & & & I & \\ & & & & U \end{pmatrix}$$

属于 $\mathfrak{T}$.

【证】 设 p 是 ν 维向量, 而 $q = 2(p\Delta p')^{-1}p$, 我们就有下面的等式:

$$\begin{pmatrix} 1 & & -\frac{1}{2}p\Delta p' & & -p \\ & I & & & \\ & & 1 & & \\ & & & I & \\ & & \Delta p' & & I \end{pmatrix} \begin{pmatrix} 1 & & & & \\ & I & & & \\ -\frac{1}{2}q\Delta q' & & 1 & & -q \\ & & & I & \\ -\Delta q' & & & & I \end{pmatrix}$$

$$\cdot \begin{pmatrix} 1 & & -\frac{1}{2}p\Delta p' & & -p \\ & I & & & \\ & & 1 & & \\ & & & I & \\ & & \Delta p' & & I \end{pmatrix}$$

$$= \begin{pmatrix} 0 & & -\frac{1}{2}p\Delta p' & & \\ & I & & & \\ -2(p\Delta p')^{-1} & & 0 & & \\ & & & I & \\ & & & & I - 2(p\Delta p')^{-1}\Delta p'p \end{pmatrix}.$$

值得注意的是, $I - 2(p\Delta p')^{-1}\Delta p'p$ 是以 p 为非迷向向量的对称. 因为任意的 $U \in Q_{n-2\nu}(F, \Delta)$ 都可以表成对称之积, 所以从上面这个等式马上就可以推出这个定理来.

我们还可以说, 当 $|U| = 1$ 时, 我们有第一种情形发生, 而当 $|U| = -1$ 时, 我们有第二种情形发生.

定理 4 当 $\nu \geqslant 2$ 时, $\Omega_n(F, S) = \mathfrak{T}$.

【证】 因为

$$\begin{pmatrix} 1 & 1 \\ & 1 \end{pmatrix} = \begin{pmatrix} 1 & -1 \\ & 1 \end{pmatrix} \begin{pmatrix} 1 & \\ & 1/2 \end{pmatrix} \begin{pmatrix} 1 & -1 \\ & 1 \end{pmatrix}^{-1} \begin{pmatrix} 1 & \\ & 1/2 \end{pmatrix}^{-1},$$

所以 2 平延 (3) 是 $O_n(F,S)$ 里元素的换位子, 因此每个 2 平延都是 $O_n(F,S)$ 里元素的换位子, 所以 $\mathfrak{T} \subseteq \Omega_n(F,S)$.

反过来, 我们还需证明 $\Omega_n(F,S) \subseteq \mathfrak{T}$.

因为 $\mathfrak{T}$ 是 $O_n(F,S)$ 的正规子群, 所以根据定理 1.2, 定理 1.3, 定理 2, 定理 3, 我们可以把 $O_n(F,S)$ 里任意两个元素 A 和 B 写成

$$A = \begin{pmatrix} a & & & & \\ & I & & & \\ & & a^{-1} & & \\ & & & I & \\ & & & & I \end{pmatrix} A_1 \text{ 或 } \begin{pmatrix} & & a & & \\ & I & & & \\ a^{-1} & & & & \\ & & & I & \\ & & & & I \end{pmatrix} A_1,$$

$$B = \begin{pmatrix} b & & & & \\ & I & & & \\ & & b^{-1} & & \\ & & & I & \\ & & & & I \end{pmatrix} B_1 \text{ 或 } \begin{pmatrix} & & b & & \\ & I & & & \\ b^{-1} & & & & \\ & & & I & \\ & & & & I \end{pmatrix} B_1,$$

而 A_1 和 B_1 都是 $\mathfrak{T}$ 里的元素. 于是

$$ABA^{-1}B^{-1} = \begin{pmatrix} \lambda^2 & & & & \\ & I & & & \\ & & \lambda^{-2} & & \\ & & & I & \\ & & & & I \end{pmatrix} T,$$

而 T 是 $\mathfrak{T}$ 里的元素, $\lambda = (aba^{-1}b^{-1})^{1/2}, a, b^{-1}$ 或 ab^{-1}. 由定理 2,

$$\begin{pmatrix} \lambda^2 & & & & \\ & I & & & \\ & & \lambda^{-2} & & \\ & & & I & \\ & & & & I \end{pmatrix}$$

属于 $\mathfrak{T}$, 所以 $ABA^{-1}B^{-1} \in \mathfrak{T}$. 这就证明了 $\Omega_n(F,S) \subseteq \mathfrak{T}$.

定理 5 当 $\nu \geqslant 2$ 时, $\Omega_n(F,S)$ 的中心即是 $\Omega_n(F,S) \cap Z_n$.

可仿照第八章定理 2.2 证之.

§3　由双曲旋转的平方所演成的群

定义　设 $\nu \geqslant 1$. 如果一个非迷向的平面 P(即 2 维子空间) 含有两个不相正交的迷向向量, 我们就把它叫双曲平面. $O_n(F,S)$ 里的一个元素叫做以 P 为双曲平面以 P^* 为轴的双曲运动, 如果它不变 P^* 里每一个向量, 同时它把 P 里的向量仍然变成 P 里的向量; 如果除此之外, 这个元素还属于 $O_n^+(F,S)$, 我们就把它叫做双曲旋转.

定理 1　设 $\nu \geqslant 1$. 在 $O_n(F,S)$ 之下, 双曲运动 R 一定相似于下面形状的一个元素:

$$(1)\qquad \begin{pmatrix} a & & & & \\ & I & & & \\ & & a^{-1} & & \\ & & & I & \\ & & & & I \end{pmatrix} \text{ 或 } \begin{pmatrix} & & a & & \\ & I & & & \\ a^{-1} & & & & \\ & & & I & \\ & & & & I \end{pmatrix}.$$

如果 R 是双曲旋转, 它就一定相似于前者.

【证】　设 P 是 R 的平面, v_1 和 v_2 是 P 里两个不相正交的迷向向量, 我们可以假定 $v_1Sv_2'=1$. 于是

$$\begin{pmatrix} v_1 \\ v_2 \end{pmatrix} S \begin{pmatrix} v_1 \\ v_2 \end{pmatrix}' = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}.$$

令

$$P_1 = \begin{pmatrix} 1 & 0^{(1,\nu-1)} & 1 & 0^{(1,\nu-1)} & 0^{(1,n-2\nu)} \\ 0 & 0 & 0 & 0 & 0 \end{pmatrix},$$

则

$$P_1SP_1' = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}.$$

依定理 1.1 就有一个正交阵 T 存在, 使

$$\begin{pmatrix} v_1 \\ v_2 \end{pmatrix} = P_1T.$$

于是 TRT^{-1} 就是以 P_1 为平面的双曲运动, 显然 TRT^{-1} 取定理所要证明的形状.

在本节以下一部分我们总假定 $\nu=1$ 和 $F \neq F_3$. 我们用 $\mathfrak{H}$ 来表示 $O_n(F,S)$ 中双曲旋转的平方所演成的群. 显然, $\mathfrak{H}$ 是 $O_n(F,S)$ 的正规子群.

定理 2　当 $\nu=1$ 及 $F \neq F_3$ 时, 以下这些元素都是 $\mathfrak{H}$ 里的元素:

$$(2) \qquad \begin{pmatrix} a^2 & & \\ & a^{-2} & \\ & & I \end{pmatrix},$$

其中 a 是 F 里任意 $\neq 0$ 的元素;

$$(3) \qquad \begin{pmatrix} 1 & -\frac{1}{2}p\Delta p' & -p \\ & 1 & \\ & \Delta p' & I \end{pmatrix} \text{和} \begin{pmatrix} & 1 & \\ -\frac{1}{2}p\Delta p' & 1 & -p \\ \Delta p' & & I \end{pmatrix},$$

其中 p 是任意的 $n-2$ 维向量.

【证】 因为 (2) 是双曲旋转的平方, 所以属于 $\mathfrak{H}$. 又因为 $F \neq F_3$, 所以我们可以在 F 里选取一个元素 $a \neq 0$, 使 $a^2 \neq 1$, 那么从

$$(4) \quad \begin{pmatrix} a^2 & & \\ & a^{-2} & \\ & & I \end{pmatrix}\begin{pmatrix} 1 & -\frac{1}{2}p\Delta p' & -p \\ & 1 & \\ & \Delta p' & I \end{pmatrix}\begin{pmatrix} a^2 & & \\ & a^{-2} & \\ & & I \end{pmatrix}^{-1}\begin{pmatrix} 1 & -\frac{1}{2}p\Delta p' & -p \\ & 1 & \\ & \Delta p' & I \end{pmatrix}^{-1}$$

$$= \begin{pmatrix} 1 & -\frac{1}{2}(1-a^2)^2 p\Delta p' & (1-a^2)p \\ & 1 & \\ & -(1-a^2)\Delta p' & I \end{pmatrix}$$

就可以推出 (3) 也属于 $\mathfrak{H}$.

和定理 2.3 完全一样, 我们可以证明下面的

定理 3 给了任意一个 $U \in O_{n-2}(F, \Delta)$, F 里就有一个元素 $a \neq 0$ 存在, 使

$$(5) \qquad \begin{pmatrix} a & & \\ & a^{-1} & \\ & & U \end{pmatrix} \quad \text{或} \quad \begin{pmatrix} & a & \\ a^{-1} & & \\ & & U \end{pmatrix}$$

属于 $\mathfrak{H}$.

从这个定理我们可以推出

定理 4 当 $n \geqslant 3$, $\nu = 1$ 及 $F \neq F_3$ 时, $\Omega_n(F, S) = \mathfrak{H}$.

【证】 因为

$$\begin{pmatrix} a^2 & \\ & a^{-2} \end{pmatrix} = \begin{pmatrix} a & \\ & a^{-1} \end{pmatrix}\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}\begin{pmatrix} a & \\ & a^{-1} \end{pmatrix}^{-1}\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}^{-1},$$

所以 $\mathfrak{H} \subseteq \Omega_n(F, S)$. 至于 $\Omega_n(F, S) \subseteq \mathfrak{H}$ 的证明是和定理 3.4 中 $\Omega_n(F, S) \subseteq \mathfrak{T}$ 的证明一样, 我们就不重复了.

如果要包括 $F = F_3$ 的情形, 我们可以证明下面的

定理 5 当 $n\geqslant 3$ 及 $\nu=1$ 时, $\Omega_n(F,S)$ 是由所有形状 (3) 的元素在 $O_n(F,S)$ 里演成的正规子群. 同时, 给了任意 $U\in O_{n-2}(F,\Delta)$, F 里就有一个元素 $a\neq 0$ 存在, 使 (5) 属于 $\Omega_n(F,S)$.

【证】 用 $\mathfrak{N}$ 表示由所有形状 (3) 的元素在 $O_n(F,S)$ 里演成的正规子群. 我们先证明 $\mathfrak{N}\subseteq\Omega_n(F,S)$. 这是显然的, 因为

$$\begin{pmatrix} 1 & -\frac{1}{2}p\Delta p' & -p \\ & 1 & \\ & \Delta p' & I \end{pmatrix} = \begin{pmatrix} 1 & -\frac{1}{8}p\Delta p' & -\frac{1}{2}p \\ & 1 & \\ & \frac{1}{2}\Delta p' & I \end{pmatrix}\begin{pmatrix} 1 & & \\ & 1 & \\ & & -I \end{pmatrix}$$

$$\cdot\begin{pmatrix} 1 & -\frac{1}{8}p\Delta p' & -\frac{1}{2}p \\ & 1 & \\ & \frac{1}{2}\Delta p' & I \end{pmatrix}\begin{pmatrix} 1 & & \\ & 1 & \\ & & -I \end{pmatrix}^{-1}.$$

至于 $\Omega_n(F,S)\subseteq\mathfrak{N}$ 的证明和这个定理中最后一句断言的证明分别和定理 2.4 及定理 2.3 的一样, 在此就不重复了.

定理 6 当 $n\geqslant 3$ 及 $\nu=1$ 时, $\Omega_n(F,S)$ 的中心即是 $\Omega_n(F,S)\cap Z_n$.

仍像定理 2.5 一样, 可以仿照第八章定理 2.2 证之.

§4 $O_n^+(F,S)/\Omega_n(F,S)$ 的构造 $(n=2\nu)$

在本节中我们假定 $n=2\nu\geqslant 4$, 于是

$$S=\begin{pmatrix} 0 & I^{(\nu)} \\ I^{(\nu)} & 0 \end{pmatrix}.$$

我们平行于第八章 §5 ~ §6 节来讨论商群 $O_n^+(F,S)/\Omega_n(F,S)$ 的构造.

依定理 1.2, $O_n(F,S)$ 中任一矩阵 Σ 皆可表成形状

$$(1)\qquad \Sigma=\begin{pmatrix} I & \\ X & I \end{pmatrix}\begin{pmatrix} A & \\ & A'^{-1} \end{pmatrix}\begin{pmatrix} I & Y \\ & I \end{pmatrix}\begin{pmatrix} I-J & J \\ J & I-J \end{pmatrix},$$

其中 X,Y 是斜对称矩阵, A 是可逆矩阵, 而 $J_2=J$ 是对角形矩阵. 因此 Σ 也可表作

$$(2)\qquad \Sigma=\begin{pmatrix} A & B \\ C & D \end{pmatrix}\begin{pmatrix} I-J & J \\ J & I-J \end{pmatrix},$$

其中 A 可逆而 $J^2=J$ 是对角形矩阵, 显而易见 $\Sigma\in O_n^+(F,S)$ 当且仅当 J 的秩是偶数.

定理 1　如果有两种方法将 $O_n^+(F,S)$ 中一个元素 Σ 表成形状 (2):

$$(3)\quad \sum = \begin{pmatrix} A & B \\ C & D \end{pmatrix}\begin{pmatrix} I-J & J \\ J & I-J \end{pmatrix} = \begin{pmatrix} A_1 & B_1 \\ C_1 & D_1 \end{pmatrix}\begin{pmatrix} I-J_1 & J_1 \\ J_1 & I-J_1 \end{pmatrix},$$

其中 $\det A \neq 0, \det A_1 \neq 0$, 而 J 和 J_1 的秩都是偶数, 那么 $\det A \cdot \det A_1 \in F^{*2}, F^{*2}$ 是 F^* 中平方元素所组成的群.

【证】　令 $J_2 = J + J_1 - 2JJ_1$, 即 J_2 的秩也是偶数. 由 (3) 式得

$$\begin{pmatrix} A_1 & B_1 \\ C_1 & D_1 \end{pmatrix} = \begin{pmatrix} A & B \\ C & D \end{pmatrix}\begin{pmatrix} I-J_2 & J_2 \\ J_2 & I-J_2 \end{pmatrix}.$$

于是

$$A_1 = A(I-J_2) + BJ_2 = A(I - J_2 + A^{-1}BJ_2);$$

因此

$$\begin{aligned}\det A_1 =& \det A \det(I - J_2 + A^{-1}BJ_2)\\ =& \det A \det(I - J_2 + J_2A^{-1}BJ_2).\end{aligned}$$

因 $A^{-1}B$ 斜对称, 故 $J_2A^{-1}BJ_2$ 亦然; 因此 $\det(I - J_2 + J_2A^{-1}BJ_2)$ 是 F^* 中平方元素, 故 $\det A \det A_1 \in F^{*2}$.

系理　如果将 $O_n^+(F,S)$ 中一个元素 Σ 表成如形状 (2), 其中 $\det A \in F^{*2}$, 而 J 的秩是偶数, 那么 Σ 的任何另一表成形状 (2) 的表法也有此性质.

我们以 $O_n'(F,S)$ 表具有系理中所说的性质的正交矩阵的集合.

基于定理 1, 我们可以定义一个从 $O_n^+(F,S)$ 到 F^*/F^{*2} 之上的映射如下: 即如 $\Sigma \in O_n^+(F,S)$, 而将 Σ 表成形状 (2), 那么定义

$$\Psi : \sum \to \det AF^{*2}.$$

以下我们要证明 Ψ 是个同态映射, 而 $\Omega_n(F,S)$ 是它的核.

平行于第八章引理 5.1~5.3, 我们也有

引理 1　设 X, Y, Z 都是 $\nu \times \nu$ 斜对称矩阵, 则

$$\begin{pmatrix} I & Y \\ & I \end{pmatrix}\begin{pmatrix} I & \\ X & I \end{pmatrix}\begin{pmatrix} I & Z \\ & I \end{pmatrix} \in O_n'(F,S).$$

引理 2　设 A 是 $\nu\times\nu$ 可逆矩阵, 设 $i_1, i_2, \cdots, i_\nu$和$j_1, j_2, \cdots, j_\nu$ 都是 $1, 2, \cdots, \nu$ 的排列, 而且 $1 \leqslant i_1 < i_2 < \cdots < i_r \leqslant \nu, 1 \leqslant i_{r+1} < \cdots < i_\nu \leqslant \nu, 1 \leqslant j_1 < \cdots < j_r \leqslant \nu, 1 \leqslant j_{r+1} < \cdots < j_\nu \leqslant \nu$. 以 $A\begin{pmatrix} i_1 \cdots i_r \\ j_1 \cdots j_r \end{pmatrix}$ 表 A 中位于 (i_k, j_l) $(k, l = 1, \cdots, r)$

位置的元素所组成的子式, 对于

$$A'^{-1}\begin{pmatrix} i_{r+1}\cdots i_\nu \\ j_{r+1}\cdots j_\nu \end{pmatrix}$$

也有同样的意义. 设

$$A\begin{pmatrix} i_1\cdots i_r \\ j_1\cdots j_r \end{pmatrix}\neq 0,$$

则

$$\operatorname{sgn}\begin{pmatrix} i_1\cdots i_\nu \\ j_1\cdots j_\nu \end{pmatrix} A\begin{pmatrix} i_1\cdots i_r \\ j_1\cdots j_r \end{pmatrix} A'^{-1}\begin{pmatrix} i_{r+1}\cdots i_\nu \\ j_{r+1}\cdots j_\nu \end{pmatrix}\det A\in F^{*2},$$

其中

$$\operatorname{sgn}\begin{pmatrix} i_1\cdots i_\nu \\ j_1\cdots j_\nu \end{pmatrix}=\begin{cases} 1 & \text{如}\begin{pmatrix} i_1\cdots i_\nu \\ j_1\cdots j_\nu \end{pmatrix}\text{是偶置换}, \\ -1 & \text{如}\begin{pmatrix} i_1\cdots i_\nu \\ j_1\cdots j_\nu \end{pmatrix}\text{是奇置换}. \end{cases}$$

特别, 如 $\det A\in F^{*2}$, 则

$$\operatorname{sgn}\begin{pmatrix} i_1\cdots i_\nu \\ j_1\cdots j_\nu \end{pmatrix} A\begin{pmatrix} i_1\cdots i_r \\ j_1\cdots j_r \end{pmatrix} A'^{-1}\begin{pmatrix} i_{r+1}\cdots i_\nu \\ j_{r+1}\cdots j_\nu \end{pmatrix}\in F^{*2}.$$

引理 3 设 $J^2=J$ 和 $J_1^2=J_1$ 都是对角形矩阵, 则

$$\begin{pmatrix} I-J & J \\ J & I-J \end{pmatrix}\begin{pmatrix} I-J_1 & J_1 \\ J_1 & I-J_1 \end{pmatrix}=\begin{pmatrix} I-J_2 & J_2 \\ J_2 & I-J_2 \end{pmatrix}$$

其中 $J_2=J+J_1-2JJ_1$, 而 J_2 的秩为偶数当且仅当 J 和 J_1 的秩同时为偶数或同时为奇数.

由于这三个引理的证明与第八章引理 5.1 ~ 5.3 的证明完全相仿, 因而略去.

基于这三个引理, 我们可以依次推出以下诸事实 (以下 $J,J_1,J_2,\cdots$ 皆为对角形幂等矩阵).

I. 设 A 为可逆阵. 表

$$\begin{pmatrix} I-J & J \\ J & I-J \end{pmatrix}\begin{pmatrix} A & 0 \\ 0 & A'^{-1} \end{pmatrix}=\begin{pmatrix} A_1 & B_1 \\ C_1 & D_1 \end{pmatrix}\begin{pmatrix} I-J_1 & J_1 \\ J_1 & I-J_1 \end{pmatrix},$$

其中 $\det A_1\neq 0$, 则 J 和 J_1 的秩同为奇数或同为偶数, 而 $\det A\det A_1\in F^{*2}$.

II. 设 Y 是 $\nu\times\nu$ 斜对称矩阵, 将

$$\Sigma=\begin{pmatrix} I-J & J \\ J & I-J \end{pmatrix}\begin{pmatrix} I & Y \\ 0 & I \end{pmatrix}$$

表成形状 (2):

$$\Sigma=\begin{pmatrix} I+(I-J)YJ & * \\ * & * \end{pmatrix}\begin{pmatrix} I-J & J \\ J & I-J \end{pmatrix},$$

则 $\det(I+(I-J)YJ)=1$.

III. 设 X 是 $\nu\times\nu$ 斜对称矩阵, 将

$$\Sigma=\begin{pmatrix} I-J & J \\ J & I-J \end{pmatrix}\begin{pmatrix} I & 0 \\ X & I \end{pmatrix},$$

表成形状 (2):

$$\Sigma=\begin{pmatrix} I+JX(I-J) & * \\ * & * \end{pmatrix}\begin{pmatrix} I-J & J \\ J & I-J \end{pmatrix}$$

则 $\det(I+JX(I-J))=1$.

IV. 设 $O_n^+(F,S)$ 有两个元素

$$\Sigma=\begin{pmatrix} A & B \\ C & D \end{pmatrix},\quad \Sigma_1=\begin{pmatrix} A_1 & B_1 \\ C_1 & D_1 \end{pmatrix},$$

其中 $\det A\neq 0,\det A_1\neq 0$. 若将这两个元素的乘积表成形状 (2):

$$\Sigma\Sigma_1=\begin{pmatrix} A_2 & B_2 \\ C_2 & D_2 \end{pmatrix}\begin{pmatrix} I-J_2 & J_2 \\ J_2 & I-J_2 \end{pmatrix},$$

则 J 的秩为偶数, 而 $\det A\det A_2\in F^{*2}$.

V. 设有 $O_n^+(F,S)$ 中的元素

$$\Sigma=\begin{pmatrix} A & B \\ C & D \end{pmatrix},$$

其中 $\det A\neq 0$. 若将 Σ^{-1} 表成形状 (2):

$$\Sigma^{-1}=\begin{pmatrix} A_1 & B_1 \\ C_1 & D_1 \end{pmatrix}\begin{pmatrix} I-J_1 & J_1 \\ J_1 & I-J_1 \end{pmatrix},$$

则 J_1 的秩是偶数, 而 $\det A \det A_1 \in F^{*2}$.

VI. 设有 $O_n(F,S)$ 中元素

$$\Sigma = \begin{pmatrix} I-J & J \\ J & I-J \end{pmatrix} \begin{pmatrix} A & B \\ C & D \end{pmatrix},$$

其中 $\det A \neq 0$. 若将 Σ 表成形状 (2):

$$\Sigma = \begin{pmatrix} A_1 & B_1 \\ C_1 & D_1 \end{pmatrix} \begin{pmatrix} I-J_1 & J_1 \\ J_1 & I-J_1 \end{pmatrix},$$

则 J_1 的秩与 J 的秩同为偶数或奇数, 而 $\det A \det A_1 \in F^{*2}$.

利用以上诸事实, 与第八章定理 5.2 相平行, 可以证明

定理 2 设 $n=2\nu \geqslant 4$. 设 $\Sigma \in O_n^+(F,S)$, 表 Σ 成形状 (2):

(2) $$\Sigma = \begin{pmatrix} A & B \\ C & D \end{pmatrix} \begin{pmatrix} I-J & J \\ J & I-J \end{pmatrix},$$

其中 $\det A \neq 0$. 于是从 $O_n^+(F,S)$ 到 F^*/F^{*2} 中的映射

(4) $$\Psi: \quad \Sigma \to \det AF^{*2}$$

是从 $O_n^+(F,S)$ 到 F^*/F^{*2} 之上的同态映射, 它的核是 $O_n'(F,S)$. 因此

$$O_n^+(F,S)/O_n'(F,S) \approx F^*/F^{*2}.$$

定理 3 设 $n=2\nu \geqslant 4$. 则 $O_n'(F,S)$ 是 $O_n(F,S)$ 的换位子群, 即 $O_n'(F,S) = \Omega_n(F,S)$. 因此

$$O_n^+(F,S)/\Omega_n(F,S) \approx F^*/F^{*2}.$$

更进一步, $\Omega_n(F,S)$ 也是 $O_n^+(F,S)$ 的换位子群.

【证】 先证 $O_n'(F,S)$ 是 $O_n(F,S)$ 的正规子群. 根据定理 2, $O_n'(F,S)$ 是 $O_n^+(F,S)$ 的是正规子群. 因为 $O_n^+(F,S)$ 是 $O_n(F,S)$ 的指数 2 的子群, 而且如果 $J_1=[1,0,\cdots,0]$, 则

$$\begin{pmatrix} I-J_1 & J_1 \\ J_1 & I-J_1 \end{pmatrix} \notin O_n^+(F,S)$$

因此只要证明, 对任意 $\Sigma \in O_n'(K,S)$,

$$\Sigma_1 \begin{pmatrix} I-J_1 & J_1 \\ J_1 & I-J_1 \end{pmatrix} \Sigma \begin{pmatrix} I-J_1 & J_1 \\ J_1 & I-J_1 \end{pmatrix}^{-1} \in O_n'(F,S)$$

即可. 写

$$\Sigma = \begin{pmatrix} A & B \\ C & D \end{pmatrix} \begin{pmatrix} I-J & J \\ J & I-J \end{pmatrix},$$

其中 $\det A \in F^{*2}$ 而 $J^2 = J$ 是对角形的秩为偶数的矩阵. 于是根据 VI,

$$\Sigma_1 = \begin{pmatrix} I-J_1 & J_1 \\ J_1 & I-J_1 \end{pmatrix}\begin{pmatrix} A & B \\ C & D \end{pmatrix}\begin{pmatrix} I-J & J \\ J & I-J \end{pmatrix}\begin{pmatrix} I-J_1 & J_1 \\ J_1 & I-J_1 \end{pmatrix}^{-1}$$
$$= \begin{pmatrix} A_1 & B_1 \\ C_1 & D_1 \end{pmatrix}\begin{pmatrix} I-J_2 & J_2 \\ J_2 & I-J_2 \end{pmatrix}\begin{pmatrix} I-J & J \\ J & I-J \end{pmatrix}\begin{pmatrix} I-J_1 & J_1 \\ J_1 & I-J_1 \end{pmatrix},$$

其中 $\det A_1 \in F^{*2}$ 而 J_2 的秩是奇数. 再根据引理 3,

$$\Sigma_1 = \begin{pmatrix} A_1 & B_1 \\ C_1 & D_1 \end{pmatrix}\begin{pmatrix} I-J_3 & J_3 \\ J_3 & I-J_3 \end{pmatrix}.$$

因为 J_2, J_1 的秩是奇数而 J 的秩是偶数, 所以 J_3 的秩是偶数. 因此 $\Sigma_1 \in O_n'(F,S)$. 因此 $O_n'(F,S)$ 是 $O_n(F,S)$ 的正规子群.

其次, 利用 $O_n'(F,S)$ 是 $O_n(F,S)$ 的正规子群这一事实及 $O_n(F,S)$ 中元素的表示法 (2), 即可推出 $O_n(F,S)$ 中任意二元素的换位子皆属于 $O_n'(F,S)$. 这证明了 $\Omega_n(F,S) \subseteq O_n'(F,S)$.

最后, 我们来证明, 以 $\mathfrak{C}$ 表 $O_n^+(F,S)$ 的换位子群, 则 $O_n'(F,S) \subset \mathfrak{C}$. 为书写简便起见, 设 $n=4$. 因 $SL_2(F)$ 是 $GL_2(F)$ 的换位子群, 故当 $\det A = 1$ 时,

$$\begin{pmatrix} A & 0 \\ 0 & A'^{-1} \end{pmatrix} \in \mathfrak{C}.$$

再由

$$\begin{pmatrix} A & 0 \\ 0 & A'^{-1} \end{pmatrix}\begin{pmatrix} I & Y \\ & I \end{pmatrix}\begin{pmatrix} A & 0 \\ 0 & A'^{-1} \end{pmatrix}^{-1}\begin{pmatrix} I & Y \\ & I \end{pmatrix}^{-1} = \begin{pmatrix} I & AYA'-Y \\ & I \end{pmatrix}$$

推出

$$\begin{pmatrix} I & Y \\ & I \end{pmatrix} \in \mathfrak{C},$$

对于一切斜对称的 Y. 令 $K = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}$, 则

$$\begin{pmatrix} 0 & I \\ I & 0 \end{pmatrix} = \begin{pmatrix} I & K \\ & I \end{pmatrix}\begin{pmatrix} I & \\ K & I \end{pmatrix}\begin{pmatrix} I & K \\ & I \end{pmatrix}\begin{pmatrix} -K & \\ & -K \end{pmatrix}$$

和

$$\begin{pmatrix} \lambda^2 & & & \\ & 1 & & \\ & & \lambda^{-2} & \\ & & & 1 \end{pmatrix}$$

$$= \begin{pmatrix} \lambda & & & \\ & 1 & & \\ & & \lambda^{-1} & \\ & & & 1 \end{pmatrix} \begin{pmatrix} 0 & I \\ I & 0 \end{pmatrix} \begin{pmatrix} \lambda & & & \\ & 1 & & \\ & & \lambda^{-1} & \\ & & & 1 \end{pmatrix}^{-1} \begin{pmatrix} 0 & I \\ I & 0 \end{pmatrix}^{-1}$$

都属于 $\mathfrak{C}$. 因此 $O_n'(F,S) \subset \mathfrak{C}$.

综合以上, 就推出 $O_n'(F,S)$ 是 $O_n(F,S)$ 的换位子群, 也是 $O_n^+(F,S)$ 的换位子群.

§5 $O_n^+(F,S)/\Omega_n(F,S)$ 的构造 $(n>2\nu)$

定理 1 设 $n \geqslant 3$ 及 $\nu \geqslant 1$. 则 $O_n(F,S)$ 里的每个元素 T 都可表成下面形状:

$$T = H\Gamma,$$

这里 Γ 是 $\Omega_n(F,S)$ 里的元素, 而 H 是以一个预先给定的双曲平面 P 为平面的双曲运动, 当 T 属于 $O_n^+(F,S)$ 时, H 就是双曲旋转.

【证】 根据定理 1.2, 1.3, 2.2, 2.3, 3.5, 我们可以把 T 写成

$$T = H_1\Gamma_1, \quad H_1 = \begin{pmatrix} a & & & & \\ & I & & & \\ & & a^{-1} & & \\ & & & I & \\ & & & & I \end{pmatrix} \text{或} \begin{pmatrix} & & a & & \\ & I & & & \\ a^{-1} & & & & \\ & & & I & \\ & & & & I \end{pmatrix},$$

而 Γ_1 是 $\Omega_n(F,S)$ 里的元素. 设 R 是把双曲面 P_1 变到 P 去的正交矩阵, 那么 $H = R^{-1}H_1R$ 就是以 P 为平面的双曲运动, 而

$$T = H_1\Gamma_1 = HH^{-1}H_1\Gamma_1 = HR^{-1}H_1^{-1}RH_1\Gamma_1 = H\Gamma,$$

这里 $\Gamma = R^{-1}H_1^{-1}RH_1\Gamma_1$ 是 $\Omega_n(F,S)$ 里的元素. 这就证明了定理.

系理 设 $n \geqslant 3$ 及 $\nu \geqslant 1$. 则在 $\Omega_n(F,S)$ 之下, 双曲运动仍和形状 (3.1) 的一个双曲运动相似.

这是定理 3.1 和定理 5.1 的直接推论.

定理 2　设 $n \geqslant 5$ 及 $\nu \geqslant 2$. 则在 $\Omega_n(F,S)$ 之下, 2 平延既相似于形状

$$(1)\qquad \begin{pmatrix} A & & \\ & A'^{-1} & \\ & & I \end{pmatrix},\quad A = \begin{pmatrix} 1 & a & \\ & 1 & \\ & & I \end{pmatrix}$$

的一个元素, 又相似于形状

$$(2)\qquad \begin{pmatrix} 1 & K & \\ & I & \\ & & I \end{pmatrix},\quad K = \begin{pmatrix} & a & \\ -a & & \\ & & 0 \end{pmatrix}$$

的一个元素. 当 $\nu \geqslant 3$ 时, 我们还可以假定 $a = 1$.

【证】　设 T 是 2 平延, 依定理 2.1, 我们可以找到一个正交矩阵 P, 使 PTP^{-1} 取形状 (1). 因为 $n \geqslant 5$, 所以我们不妨假定 $P \in O_n^+(F,S)$. 于是, 依定理 5.1, 我们可以把 P 写成

$$P = \begin{pmatrix} I & & & & \\ & a & & & \\ & & I & & \\ & & & a^{-1} & \\ & & & & I \end{pmatrix} \Gamma,$$

而 $\Gamma \in \Omega_n(F,S)$. 于是 $\Gamma T \Gamma^{-1}$ 就是形式 (1) 的元素了. 我们还可以用同样的方法来对待 (2).

§6　$P\Omega_n(F,S)$ 是单群的证明

定理 1　设 $n \geqslant 3$ 及 $\nu \geqslant 1$. 那么除了下面两个例外情形之外, $P\Omega_n(F,S)$ 总是单群, 而这两个例外情形是:

$$\text{I. } P\Omega_4\left(F, \begin{pmatrix} 0 & I^{(2)} \\ I^{(2)} & 0 \end{pmatrix}\right),$$

$$\text{II. } P\Omega_3\left(F_3, \begin{pmatrix} 0 & 1 & \\ 1 & 0 & \\ & & 1 \end{pmatrix}\right).$$

我们略去

$$P\Omega_4\left(F,\begin{pmatrix}0&I\\I&0\end{pmatrix}\right),P\Omega_3\left(F_3,\begin{pmatrix}0&1&\\1&0&\\&&1\end{pmatrix}\right) 和\ P\Omega_4\left(F_3,\begin{pmatrix}0&1&&\\1&0&&\\&&1&\\&&&1\end{pmatrix}\right)$$

这三个情形的讨论, 它们可以在 Dickson, Linear groups 一书中找到. 这里我们只证明除了这几个例外情形之外, $P\Omega_n(F,S)$ 总是单群. 又因为当 $n\geqslant 5$ 时, F_3 上 n 行 n 列可逆对称矩阵的指数总是 >1 的, 所以我们只要就下面的两种情形证明 $P\Omega_n(F,S)$ 是单群就行了, 这两种情形是:

I. $\nu=1,n\geqslant 3$ 及 $F\neq F_3$;

II. $\nu\geqslant 2,n\geqslant 5$.

在这一节里我们将研究第一种情形, 总假定 $\nu=2,n\geqslant 3$ 及 $F\neq F_3$.

引理 1 设 $\nu=1,n\geqslant 3$ 及 $F\neq F_3$. 如果 $\Omega_n(F,S)$ 的一个正规子群 $\mathfrak{N}$ 包有下面形状的一个元素:

$$(1)\qquad \begin{pmatrix}1&-\frac{1}{2}p\Delta p'&p\\&1&\\&-\Delta p'&I\end{pmatrix},$$

而 p 是一个不等于零的 $n-2$ 维向量, 则 $\mathfrak{N}=\Omega_n(F,S)$.

【证】 对于 F 里的任意元素 $x\neq 0,\mathfrak{N}$ 总含有

$$\begin{pmatrix}1&-\frac{1}{2}x^4p\Delta p'&x^2p\\&1&\\&-\Delta x^2p&I\end{pmatrix}$$
$$=\begin{pmatrix}x^2&&\\&x^{-2}&\\&&I\end{pmatrix}\begin{pmatrix}1&-\frac{1}{2}p\Delta p'&p\\&1&\\&-\Delta p'&I\end{pmatrix}\begin{pmatrix}x^2&&\\&x^{-2}&\\&&I\end{pmatrix}^{-1},$$

因此 $\mathfrak{N}$ 就含有

$$\begin{pmatrix}1&-\frac{1}{2}(4x^2)p\Delta p'&2xp\\&1&\\&-\Delta(2x)p'&I\end{pmatrix}=\begin{pmatrix}1&-\frac{1}{2}p\Delta p'&p\\&1&\\&-\Delta p'&I\end{pmatrix}^{-1}$$
$$\cdot\begin{pmatrix}1&-\frac{1}{2}x^4\Delta p'&x^2p\\&1&\\&-\Delta x^2p'&I\end{pmatrix}^{-1}\begin{pmatrix}1&-\frac{1}{2}(x+1)^4p\Delta p'&(x+1)^2p\\&1&\\&-\Delta(x+1)^2p'&I\end{pmatrix}.$$

因为 F 的特征数 $\neq 2$, 所以当 x 跑过 F 中所有不等于零的元素时, $2x$ 也是这样. 因此, 对于 F 里任意的 $\lambda \neq 0, \mathfrak{N}$ 都含有

$$\begin{pmatrix} 1 & -\frac{1}{2}\lambda^2 p\Delta p' & \lambda p \\ & 1 & \\ & -\Delta\lambda p' & I \end{pmatrix}.$$

又因为

$$\begin{pmatrix} 0 & -\frac{1}{2}p\Delta p' & \\ -2(p\Delta p')^{-1} & 0 & \\ & & I-2(p\Delta p')^{-1}\Delta p'p \end{pmatrix}^{-1} \begin{pmatrix} 1 & -\frac{1}{2}p\Delta p' & p \\ & 1 & \\ & -\Delta p' & I \end{pmatrix}$$

$$\cdot \begin{pmatrix} 0 & -\frac{1}{2}p\Delta p' & \\ -2(p\Delta p')^{-1} & 0 & \\ & & I-2(p\Delta p')^{-1}\Delta p'p \end{pmatrix}$$

$$= \begin{pmatrix} 1 & & \\ -2(p\Delta p')^{-1} & 1 & 2(p\Delta p')^{-1}p \\ -\Delta 2(p\Delta p')^{-1}p' & & I \end{pmatrix}$$

也属于 $\mathfrak{N}$, 所以我们可以同样地证明, 对于 F 里任意的 $\lambda \neq 0, \mathfrak{N}$ 总含有

$$\begin{pmatrix} 1 & & \\ -\frac{1}{2}\lambda^2 p\Delta p' & 1 & \lambda p \\ -\Delta\lambda p' & & I \end{pmatrix}.$$

于是, 当 $q = 2\lambda^{-1}(p\Delta p')^{-1}p$ 时,

$$\begin{pmatrix} 1 & -\frac{1}{2}\lambda^2 p\Delta p' & \lambda p \\ & 1 & \\ & -\Delta\lambda p' & I \end{pmatrix} \begin{pmatrix} 1 & & \\ -\frac{1}{2}q\Delta q' & 1 & q \\ -\Delta q' & & I \end{pmatrix} \begin{pmatrix} 1 & -\frac{1}{2}\lambda^2 p\Delta p' & \lambda p \\ & 1 & \\ & -\Delta\lambda p' & I \end{pmatrix}$$

$$= \begin{pmatrix} 0 & -\frac{1}{2}\lambda^2 p\Delta p' & \\ -2(\lambda^2 p\Delta p')^{-1} & 0 & \\ & & I-2(p\Delta p')^{-1}\Delta p'p \end{pmatrix}$$

也属于 $\mathfrak{N}$. 因此 $\mathfrak{N}$ 就含有

$$(2)\ \begin{pmatrix} \lambda^2 & & \\ & \lambda^{-2} & \\ & & I \end{pmatrix} = \begin{pmatrix} 0 & -\frac{1}{2}\lambda^2 p\Delta p' & \\ -2(\lambda^2 p\Delta p')^{-1} & 0 & \\ & & I-2(p\Delta p')^{-1}\Delta p'p \end{pmatrix}$$

$$\cdot \begin{pmatrix} 0 & -\frac{1}{2}p\Delta p' & \\ -2(p\Delta p')^{-1} & 0 & \\ & & I-2(p\Delta p')^{-1}\Delta p'p \end{pmatrix},$$

而 λ 是 F 里任意 $\neq 0$ 的元素. 根据定理 5.2, 我们知道, 任意一个双曲线旋转的平方在 $\Omega_n(F,S)$ 之下都和形状 (2) 的一个元素相似, 所以 $\mathfrak{N}$ 就含有所有双曲线旋转的平方. 依定理 3.4, 我们就得到 $\mathfrak{N} = \Omega_n(F,S)$.

用同样的方法我们可以证明

引理 2 设 $\nu = 1, n \geqslant 3$ 及 $F \neq F_3$. 如果 $\Omega_n(F,S)$ 的一个正规子群 $\mathfrak{N}$ 包有下面形状的一个元素:

$$(3)\qquad \begin{pmatrix} 1 & & \\ -\frac{1}{2}q\Delta q' & 1 & q \\ -\Delta q' & & I \end{pmatrix},$$

而 q 是一个不等于零的 $n-2$ 维向量, 则 $\mathfrak{N} = \Omega_n(F,S)$.

引理 3 设 $\nu = 1, n \geqslant 3$ 及 $F \neq F_3$. 如果 $\Omega_n(F,S)$ 的一个正规子群包有一个双曲旋转的平方, 而这个平方不等于单位矩阵, 那么 $\mathfrak{N} = \Omega_n(F,S)$.

【证】 依定理 3.2, 我们可以假定 $\mathfrak{N}$ 所含的双曲旋转的平方是形状 (2) 的一个元素, 而 $\lambda^2 \neq 1$. 于是从 (3.4) 式我们就可以推出 $\mathfrak{N}$ 包有所有形如 (1) 的元素, 那么从引理 1 就可以推出我们这个引理来.

现在让我们来证明: 当 $\nu = 1, n \geqslant 3$ 及 $F \neq F_3$ 时, $P\Omega_n(F,S)$ 是单群. 证明这一点是和证明 $\Omega_n(F,S)$ 没有非中心的真正规子群是一样的. 假定 $\mathfrak{N}$ 是 $\Omega_n(F,S)$ 的任意一个非中心的正规子群, 我们将要证明 $\mathfrak{N} = \Omega_n(F,S)$, 这样就证明了 $P\Omega_n(F,S)$ 是单群.

设 $\mathfrak{N}$ 含有一个非中心的元素 A, 那么 $A \neq \pm I$. 我们把 A 写作

$$A = \begin{pmatrix} a & b & p \\ c & d & q \\ r' & t' & U \end{pmatrix},$$

其中 a, b, c, d 是 F 里的元素, p, q, r, t 是 $n-2$ 维的向量, 而 U 是 $(n-2)\times(n-2)$ 矩阵.

首先, 我们研究 $b \neq 0$ 的情形. 因为 $\mathfrak{N}$ 也含有

$$\begin{pmatrix} 1 & & \\ -\frac{1}{2}x\Delta x' & 1 & x \\ -\Delta x' & & I \end{pmatrix}^{-1} \begin{pmatrix} a & b & p \\ c & d & q \\ r' & t' & U \end{pmatrix} \begin{pmatrix} 1 & & \\ -\frac{1}{2}x\Delta x' & 1 & x \\ -\Delta x' & & I \end{pmatrix}$$

$$= \begin{pmatrix} * & b & bx+p \\ * & * & * \\ * & * & * \end{pmatrix},$$

其中 * 表示没有明确地写出来的元素. 所以可选取 x, 使 $bx+p=0$. 于是我们就在 $\mathfrak{N}$ 里找到一个 $p=0$ 的元素. 从 $p=0$ 可以推出 $a=0$ 和 $r'=0$. 因此, 不失去普遍性, 可以假定

$$A = \begin{pmatrix} 0 & b & 0 \\ c & d & q \\ 0 & t' & U \end{pmatrix}.$$

我们分别来研究 $q=0$ 和 $q \neq 0$ 这两种情形.

(i) $q \neq 0$. 于是

$$A = \begin{pmatrix} 0 & b & 0 \\ b^{-1} & -\frac{1}{2}bq\Delta q' & q \\ 0 & -bU\Delta q' & U \end{pmatrix}, \text{而} U\Delta U' = \Delta.$$

那么 $\mathfrak{N}$ 就含有

$$B = A \begin{pmatrix} x^2 & & \\ & x^{-2} & \\ & & I \end{pmatrix} A^{-1} \begin{pmatrix} x^2 & & \\ & x^{-2} & \\ & & I \end{pmatrix}^{-1}$$

$$= \begin{pmatrix} x^{-4} & 0 & 0 \\ -\frac{1}{2}q\Delta q'(1-x^{-2})^2 & x^4 & (1-x^2)qU^{-1} \\ U\Delta q'(x^{-2}-x^{-4}) & 0 & I \end{pmatrix}$$

以及

$$B \begin{pmatrix} y^2 & & \\ & y^{-2} & \\ & & I \end{pmatrix} B^{-1} \begin{pmatrix} y^2 & & \\ & y^{-2} & \\ & & I \end{pmatrix}^{-1}$$

$$= \begin{pmatrix} 1 & 0 & 0 \\ -\frac{1}{2}q\Delta q'(x^2-1)^2(y^{-2}-1)^2 & 1 & (x^2-1)(y^{-2}-1)qU^{-1} \\ -U\Delta q'(x^2-1)(y^{-2}-1) & 0 & I \end{pmatrix}.$$

因为 $F \neq F_3$, 所以可以 F 里选取 $x \neq 0, y \neq 0$, 使 $x^2-1 \neq 0$ 及 $y^{-2}-1 \neq 0$. 因此 $(x^2-1)(y^{-2}-1)qU^{-1} \neq (0,0,\cdots,0)$. 这就是说, $\mathfrak{N}$ 含有一个形如 (3) 的元素. 于是, 在这种情形之下, 我们的定理可从引理 2 推出.

(ii) $q=0$. 那么 $d=0, t=0$. 于是

$$A = \begin{pmatrix} 0 & b & 0 \\ b^{-1} & 0 & 0 \\ 0 & 0 & U \end{pmatrix}.$$

分别讨论 $F \neq F_5$ 和 $F = F_5$ 这两种情形.

(ii-1) $F \neq F_5$. 我们可以在 F 里找到一个元素 $\lambda \neq 0$, 使 $\lambda^4 \neq 1$. 于是 $\mathfrak{N}$ 就含有

$$\begin{pmatrix} \lambda^2 & & \\ & \lambda^{-2} & \\ & & I \end{pmatrix}\begin{pmatrix} & b & \\ b^{-1} & & \\ & & U \end{pmatrix}\begin{pmatrix} \lambda^2 & & \\ & \lambda^{-2} & \\ & & I \end{pmatrix}^{-1}\begin{pmatrix} & b & \\ b^{-1} & & \\ & & U \end{pmatrix}^{-1} = \begin{pmatrix} \lambda^4 & & \\ & \lambda^{-4} & \\ & & I \end{pmatrix},$$

而这是一个双曲旋转的平方. 因此, 这时我们的定理可以从引理 3 推出.

(ii-2) $F = F_5$. 这里 n 只能等于 3 或者等于 4.

(ii-2-1) $n=3$. 这里 Δ 是 F 里一个不等于零的数, 而

$$A = \begin{pmatrix} & b & \\ b^{-1} & & \\ & & -1 \end{pmatrix}.$$

根据定理 2.3 的证明, 我们知道

$$\begin{pmatrix} & -\frac{1}{2}\Delta & \\ -2\Delta^{-1} & & \\ & & -1 \end{pmatrix} \in \Omega_3(F,S).$$

如果 $b^2 = \Delta^2$, 那么 $\mathfrak{N}$ 就包有下面这个双曲对合的平方：

$$\begin{pmatrix} & b & \\ b^{-1} & & \\ & & -1 \end{pmatrix}\begin{pmatrix} & -\frac{1}{2}\Delta & \\ -2\Delta^{-1} & & \\ & & -1 \end{pmatrix}\begin{pmatrix} & b & \\ b^{-1} & & \\ & & -1 \end{pmatrix}^{-1}$$

$$\cdot \begin{pmatrix} & -\frac{1}{2}\Delta & \\ -2\Delta^{-1} & & \\ & & -1 \end{pmatrix}^{-1} = \begin{pmatrix} -1 & & \\ & -1 & \\ & & 1 \end{pmatrix}.$$

因此, 在这种情形, 根据引理 3, 就有 $\mathfrak{N} = \Omega_n(F,S)$. 如果 $b^2 \neq \Delta^2$, 那么 $\mathfrak{N}$ 就含有

$$\begin{pmatrix} 1 & -\frac{1}{2}p^2\Delta & p \\ & 1 & \\ & -p\Delta & 1 \end{pmatrix}\begin{pmatrix} & b & \\ b^{-1} & & \\ & & -1 \end{pmatrix}\begin{pmatrix} 1 & -\frac{1}{2}p^2\Delta & p \\ & 1 & \\ & -p\Delta & 1 \end{pmatrix}^{-1}\begin{pmatrix} & b & \\ b^{-1} & & \\ & & -1 \end{pmatrix}^{-1}$$

$$= \begin{pmatrix} * & -\frac{1}{2}p^2\Delta & -\frac{1}{2}p^3\Delta b^{-1} + p \\ -\frac{1}{2}b^{-2}p^2\Delta & 1 & b^{-1}p \\ * & -p\Delta & -b^{-1}p^2\Delta + 1 \end{pmatrix},$$

而 p 是 F 里任意的元素. 因为 $b^2 \neq \Delta^2$, 所以 $\Delta b^{-1} = \pm 2$. 因此可在 F 里找到一个元素 $p \neq 0$, 使 $-\frac{1}{2}p^3\Delta b^{-1} + p = 0$. 于是我们就在 $\mathfrak{N}$ 里找到一个 $b \neq 0, p = 0, q \neq 0$ 的元素, 而这种情形在 (i) 里已经讨论过了.

(ii-2-2) $n = 4$. 这时

$$A = \begin{pmatrix} & b & \\ b^{-1} & & \\ & & U \end{pmatrix}, 而 |U| = -1.$$

因此 U 是一个对称, 可把 U 写成

$$U = I - 2(p\Delta p')^{-1}\Delta p'p.$$

设 q 是 p 正交的向量, 即 $p\Delta q' = 0$. 可以证明 $(p\Delta p')^2 \neq (q\Delta q')^2$. 因为, 如果不然, $p\Delta q' = \varepsilon(q\Delta q')$ 而 $\varepsilon = \pm 1$; 于是当 $\varepsilon = -1$ 时 $(p+q)\Delta(p+q)' = 0$, 而当 $\varepsilon = 1$ 时 $(p+2q)\Delta(p+2q)' = 0$. 由于 Δ 是定号的, 所以这两种情形都不可能. 因此就有 $b^2 = (p\Delta p')^2$ 或 $b^2 = (q\Delta q')^2$. 如果 $b^2 = (p\Delta p')^2$, 那么 $\mathfrak{N}$ 就含有下面这个双曲对合的平方:

$$\begin{pmatrix} & b & \\ b^{-1} & & \\ & & U \end{pmatrix}\begin{pmatrix} & -\frac{1}{2}(p\Delta p') & \\ -2(p\Delta p')^{-1} & & \\ & & U \end{pmatrix}\begin{pmatrix} & b & \\ b^{-1} & & \\ & & U \end{pmatrix}^{-1}$$

$$\cdot \begin{pmatrix} & -\frac{1}{2}p\Delta p' & \\ -2(p\Delta p')^{-1} & & \\ & & U \end{pmatrix}^{-1} = \begin{pmatrix} -1 & & \\ & -1 & \\ & & I \end{pmatrix};$$

而当 $b^2=(q\Delta q')^2$ 时, $\mathfrak{N}$ 就含有

$$\begin{pmatrix} & b & \\ b^{-1} & & \\ & & U \end{pmatrix}\begin{pmatrix} & -\frac{1}{2}(q\Delta q') & \\ -2(q\Delta q')^{-1} & & \\ & & U_1 \end{pmatrix}\begin{pmatrix} & b & \\ b^{-1} & & \\ & & U \end{pmatrix}^{-1}$$

$$\cdot\begin{pmatrix} & -\frac{1}{2}q\Delta q' & \\ -2(q\Delta q')^{-1} & & \\ & & U_1 \end{pmatrix}=\begin{pmatrix} -1 & & \\ & -1 & \\ & & I \end{pmatrix},$$

其中 $U_1=I-2(q\Delta q')^{-1}\Delta q'q$. 所以根据引理 3, 可推出 $\mathfrak{N}=\Omega_n(F,S)$.

其次, 我们来研究 $b=0$ 的情形. 如果 $c\neq 0$, 那么 $\mathfrak{N}$ 就含有

$$\begin{pmatrix} & -\frac{1}{2}(p\Delta p') & \\ -2(p\Delta p')^{-1} & & \\ & & I-2(p\Delta p')^{-1}\Delta p'p \end{pmatrix}\begin{pmatrix} a & 0 & 0 \\ c & d & q \\ r' & t' & U \end{pmatrix}$$

$$\cdot\begin{pmatrix} & -\frac{1}{2}(p\Delta p') & \\ -2(p\Delta p')^{-1} & & \\ & & I-2(p\Delta p')^{-1}\Delta p'p \end{pmatrix},$$

而这个矩阵里 $(1,2)$ 位置的元素却 $\neq 0$. 因此根据上面的推理, 就有 $\mathfrak{N}=\Omega_n(F,S)$.

如果 $b=c=0$, 那么

$$A=\begin{pmatrix} a & & \\ & a^{-1} & \\ & & U \end{pmatrix}.$$

因此 $\mathfrak{N}$ 就含有

$$\begin{pmatrix} 1 & -\frac{1}{2}p\Delta p' & p \\ & 1 & \\ & -\Delta p' & I \end{pmatrix} A \begin{pmatrix} 1 & -\frac{1}{2}p\Delta p' & p \\ & 1 & \\ & -\Delta p' & I \end{pmatrix}^{-1} A^{-1}$$

$$=\begin{pmatrix} 1 & -\frac{1}{2}(p-apU^{-1})\Delta(p-apU^{-1})' & p-apU^{-1} \\ & 1 & \\ & -\Delta(p-apU^{-1})' & I \end{pmatrix}$$

和

$$\begin{pmatrix} 1 & & \\ -\frac{1}{2}q\Delta q' & 1 & q \\ -\Delta q' & & I \end{pmatrix} A \begin{pmatrix} 1 & & \\ -\frac{1}{2}q\Delta q' & 1 & q \\ -\Delta q' & & I \end{pmatrix}^{-1} A^{-1}$$

$$= \begin{pmatrix} 1 & & \\ -\frac{1}{2}(q-a^{-1}qU^{-1})\Delta(q-a^{-1}qU^{-1}) & 1 & q-a^{-1}qU^{-1} \\ -\Delta(q-a^{-1}qU^{-1}) & & I \end{pmatrix}.$$

我们总可以找到一个 $n-2$ 维向量 p 或 q, 使 $p-apU^{-1}\neq 0$ 或 $q-a^{-1}qU^{-1}\neq 0$, 除非 $I-aU^{-1}=0$ 及 $I-a^{-1}U^{-1}=0$. 可是从 $I-aU^{-1}=0$ 和 $I-a^{-1}U^{-1}=0$ 就会推出 $U=aI=a^{-1}I$ 和 $a=a^{-1}=\pm 1$. 这就是说, $A=\pm I$, 而这和 A 的选择相抵触. 因此 $\mathfrak{N}$ 总含有一个形如 (1) 或 (3) 的元素. 根据引理 1 或 3, 就能推出 $\mathfrak{N}=\Omega_n(F,S)$.

§7　$P\Omega_n(F,S)$ 是单群的证明 (续)

在这一节里我们将证明当 $n\geqslant 5$ 和 $\nu\geqslant 2$ 时, $P\Omega_n(F,S)$ 是单群.

引理 1　设 $n\geqslant 5$ 及 $\nu\geqslant 2$. 如果 $\Omega_n(F,S)$ 的一个正规子群含有一个 2 平延, 则 $\mathfrak{N}=\Omega_n(F,S)$.

【证】　当 $\nu\geqslant 3$ 时, 根据定理 5.2, 知道 $\Omega_n(F,S)$ 里的 2 平延都是共轭的. 因此如果 $\mathfrak{N}$ 含有一个 2 平延, $\mathfrak{N}$ 就含有全部 2 平延. 于是根据定理 2.4, 就有 $\mathfrak{N}=\Omega_n(F,S)$.

当 $\nu=2$ 时, 我们可以假定 $\mathfrak{N}$ 含有 2 平延.

$$\begin{pmatrix} I & K & \\ & I & \\ & & I \end{pmatrix}, \text{而} K=\begin{pmatrix} 0 & a \\ -a & 0 \end{pmatrix}.$$

于是 $\mathfrak{N}$ 就含有

$$\begin{pmatrix} \lambda I & & \\ & \lambda^{-1}I & \\ & & I \end{pmatrix}\begin{pmatrix} I & K & \\ & I & \\ & & I \end{pmatrix}\begin{pmatrix} \lambda I & & \\ & \lambda^{-1}I & \\ & & I \end{pmatrix}^{-1}=\begin{pmatrix} I & \lambda^2 K & \\ & I & \\ & & I \end{pmatrix},$$

而 λ 是 F 里任意 $\neq 0$ 的元素. 因此 $\mathfrak{N}$ 就含有

$$\begin{pmatrix} I & \lambda^2 K & \\ & I & \\ & & I \end{pmatrix}^{-1}\begin{pmatrix} I & K & \\ & I & \\ & & I \end{pmatrix}^{-1}\begin{pmatrix} I & (\lambda+1)^2 K & \\ & I & \\ & & I \end{pmatrix}=\begin{pmatrix} I & 2\lambda K & \\ & I & \\ & & I \end{pmatrix}.$$

因为 F 的特征数 $\neq 2$, 所以当 λ 跑过 F 里所有 $\neq 0$ 的元素时, $2\lambda a$ 也跑过 F 里所有非零元素. 因此根据定理 5.2, 仍然可以推出 $\mathfrak{N}=\Omega_n(F,S)$.

引理 2 设 $n \geqslant 5$ 及 $\nu \geqslant 2$. 如果 $\Omega_n(F,S)$ 的一个正规子群 $\mathfrak{N}$ 含有一个形如

$$\begin{pmatrix} A & & \\ & A'^{-1} & \\ & & I \end{pmatrix}, \text{而} A=\begin{pmatrix} a & b & \\ -b^{-1} & 0 & \\ & & I^{(\nu-2)} \end{pmatrix} \quad (b \neq 0)$$

的元素, 那么 $\mathfrak{N}=\Omega_n(F,S)$.

【证】 因为 $SL_\nu(F)$ 不含有任何非中心真正规子群, 除非 $\nu=2$, 而且 $F=F_3$, 所以当 $\nu>2$ 或 $F \neq F_3$ 时, 这个引理从引理 1 立即推出.

当 $\nu=2$ 而且 $F=F_3$ 时, A 有六种可能性:

$$\begin{pmatrix} 1 & 1 \\ -1 & \end{pmatrix}, \begin{pmatrix} -1 & 1 \\ -1 & \end{pmatrix}, \begin{pmatrix} & 1 \\ -1 & \end{pmatrix},$$

$$\begin{pmatrix} 1 & -1 \\ 1 & \end{pmatrix}, \begin{pmatrix} -1 & -1 \\ 1 & \end{pmatrix}, \begin{pmatrix} & -1 \\ 1 & \end{pmatrix}.$$

当 $A=\begin{pmatrix} -1 & 1 \\ -1 & \end{pmatrix}$ 时, 我们有

$$\begin{pmatrix} 1 & 1 \\ -1 & 0 \end{pmatrix}^{-1}\begin{pmatrix} -1 & 1 \\ -1 & \end{pmatrix}\begin{pmatrix} 1 & 1 \\ -1 & 0 \end{pmatrix}=\begin{pmatrix} 1 & 1 \\ & 1 \end{pmatrix};$$

而当 $A=\begin{pmatrix} -1 & -1 \\ 1 & \end{pmatrix}$ 时, 我们有

$$\begin{pmatrix} & 1 \\ -1 & 1 \end{pmatrix}^{-1}\begin{pmatrix} -1 & -1 \\ 1 & \end{pmatrix}\begin{pmatrix} & 1 \\ -1 & 1 \end{pmatrix}=\begin{pmatrix} 1 & \\ 1 & 1 \end{pmatrix}.$$

于是, 在这两种情形, $\mathfrak{N}$ 总含有一个 2 平延, 因此我们的引理可从上面的引理推出.

当 $A=\begin{pmatrix} 1 & 1 \\ -1 & \end{pmatrix}$ 或 $\begin{pmatrix} 1 & -1 \\ 1 & \end{pmatrix}$ 时, $A^3=-I$; 而当 $A=\begin{pmatrix} & 1 \\ -1 & \end{pmatrix}$ 或 $\begin{pmatrix} & -1 \\ 1 & \end{pmatrix}$ 时, $A^2=-I$. 因此, 在这四种情形, $\mathfrak{N}$ 总含有

$$T=\begin{pmatrix} -I & & \\ & -I & \\ & & I \end{pmatrix}.$$

因此 $\mathfrak{N}$ 就含有

$$T^{-1}\begin{pmatrix} I & -\frac{1}{8}P\Delta P' & \frac{1}{2}P \\ & I & \\ & -\frac{1}{2}\Delta P' & I \end{pmatrix}^{-1} T \begin{pmatrix} I & -\frac{1}{8}P\Delta P' & \frac{1}{2}P \\ & I & \\ & -\frac{1}{2}\Delta P' & I \end{pmatrix}$$
$$=\begin{pmatrix} I & -\frac{1}{2}P\Delta P' & P \\ & I & \\ & -\Delta P' & I \end{pmatrix},$$

而 P 是任意 2 行 $n-4$ 列的矩阵. 于是 $\mathfrak{N}$ 就含有

$$\begin{pmatrix} I & -\frac{1}{2}P\Delta P' & P \\ & I & \\ & -\Delta P' & I \end{pmatrix}\begin{pmatrix} I & -\frac{1}{2}Q\Delta Q' & Q \\ & I & \\ & -\Delta Q' & I \end{pmatrix}.$$
$$\cdot\begin{pmatrix} I & -\frac{1}{2}(P+Q)\Delta(P+Q)' & P+Q \\ & I & \\ & -\Delta(P+Q)' & I \end{pmatrix}^{-1}$$
$$=\begin{pmatrix} I & -\frac{1}{2}P\Delta Q'+\frac{1}{2}Q\Delta P' & \\ & I & \\ & & I \end{pmatrix}.$$

我们总可以选取 P 和 Q, 使

$$-\frac{1}{2}P\Delta Q'+\frac{1}{2}Q\Delta P'=\begin{pmatrix} 0 & c \\ -c & 0 \end{pmatrix}\neq 0.$$

于是 $\mathfrak{N}$ 就含有一个 2 平延, 所以我们的引理仍然可以从引理 1 推出.

现在让我们来证明当 $n\geqslant 5$ 及 $\nu\geqslant 2$ 时, $P\Omega_n(F,S)$ 是单群. 设 $\mathfrak{N}$ 是 $\Omega_n(F,S)$ 的任意的非中心正规子群. 我们只要证明 $\mathfrak{N}=\Omega_n(F,S)$ 就行了. 因为 $\mathfrak{N}$ 是非中心的, 所以 $\mathfrak{N}$ 就含有一个非中心元素 N, 这就是说, N 不和 $\Omega_n(F,S)$ 里所有元素都交换. 因为 $\Omega_n(F,S)$ 是由 2 平延演成的, 所以就有一个 2 平延 T, 使

$$T^{-1}N^{-1}TN\neq I.$$

设

$$T=I+SP'\begin{pmatrix}0&1\\-1&0\end{pmatrix}P,$$

P 是 $2\times n$ 的矩阵, P 的秩是 2, 而且 $PSP'=0$. 那么

$$N^{-1}TN=I+S(PN)'\begin{pmatrix}0&1\\-1&0\end{pmatrix}(PN).$$

令 $PS(PN)'=M$. 考查

$$\begin{pmatrix}P\\PN\end{pmatrix}S\begin{pmatrix}P\\PN\end{pmatrix}'=\begin{pmatrix}0&M\\M'&0\end{pmatrix}.$$

我们分别来研究 M 的秩等于 2, 1 和 0 的情形.

(i) M 的秩等于 2. 这时, 有可逆矩阵 A 和 B 存在, 使

$$AMB'=\begin{pmatrix}1&0\\0&1\end{pmatrix}.$$

于是

$$\begin{pmatrix}A&\\&B\end{pmatrix}\begin{pmatrix}P\\PN\end{pmatrix}S\begin{pmatrix}P\\PN\end{pmatrix}'\begin{pmatrix}A&\\&B\end{pmatrix}'=\begin{pmatrix}0&I^{(2)}\\I^{(2)}&0\end{pmatrix}.$$

因此 $\begin{pmatrix}P\\PN\end{pmatrix}$ 的秩等于 4. 以下为书写简便起见, 把 S 写成

$$S=\begin{pmatrix}0&I^{(2)}&\\I^{(2)}&0&\\&&S_1^{(n-4)}\end{pmatrix},$$

而 S_1 当 $\nu=2$ 时是定号的, 当 $\nu\geqslant 3$ 时是不定号的. 因为

$$\begin{pmatrix}I^{(2)}&0&0^{(2,n-4)}\\0&I^{(2)}&0\end{pmatrix}S\begin{pmatrix}I^{(2)}&0&O^{(2,n-4)}\\0&I^{(2)}&0\end{pmatrix}'=\begin{pmatrix}0&I^{(2)}\\I^{(2)}&0\end{pmatrix},$$

所以根据定理 1.1, 有一个正交矩阵 R 存在, 使

$$\begin{pmatrix} I^{(2)} & 0 & O^{(2,n-4)} \\ 0 & I^{(2)} & 0 \end{pmatrix} = \begin{pmatrix} AP \\ BPN \end{pmatrix} R = \begin{pmatrix} APR \\ BPNR \end{pmatrix}.$$

于是 $R^{-1}\mathfrak{N}R$ 就含有

$$R^{-1}(T^{-1}N^{-1}TN)R = R^{-1}T^{-1}RR^{-1}(N^{-1}TN)R.$$

而

$$\begin{aligned} R^{-1}TR &= I + S(PR)'\begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}(PR) \\ &= I + S(I^{(2)},0,0)'A'^{-1}\begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}A^{-1}(I^{(2)},0,0), \end{aligned}$$

$$R^{-1}(N^{-1}TN)R = I + S(0,I,0)'B'^{-1}\begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}B^{-1}(0,I,0).$$

令 $a = |A'^{-1}|, b = |B'^{-1}|, K_1 = \begin{pmatrix} 0 & a \\ -a & 0 \end{pmatrix}$ 及 $K_2 = \begin{pmatrix} 0 & b \\ -b & 0 \end{pmatrix}$, 计算一下就得到

$$R^{-1}TR = \begin{pmatrix} I & & \\ K_1 & I & \\ & & I \end{pmatrix}, \quad R^{-1}(N^{-1}TN)R = \begin{pmatrix} I & K_2 & \\ & I & \\ & & I \end{pmatrix}.$$

因此 $R^{-1}\mathfrak{N}R$ 就含有

$$\begin{pmatrix} I & & \\ K_1 & I & \\ & & I \end{pmatrix}^{-1}\begin{pmatrix} I & K_2 & \\ & I & \\ & & I \end{pmatrix} = \begin{pmatrix} I & K_2 & \\ -K_1 & I - K_1K_2 & \\ & & I \end{pmatrix}.$$

因为 $\Omega_n(F,S)$ 是 $O_n(F,S)$ 的正规子群, $\mathfrak{N}$ 是 $\Omega_n(F,S)$ 的正规子群, 所以 $R^{-1}\mathfrak{N}R$ 也是 $\Omega_n(F,S)$ 的正规子群. 因此 $R^{-1}\mathfrak{N}R$ 就含有

$$\begin{pmatrix} I & & \\ K_1 - K_2^{-1} & I & \\ & & I \end{pmatrix}\begin{pmatrix} I & K_2 & \\ -K_1 & I - K_1K_2 & \\ & & I \end{pmatrix}\begin{pmatrix} I & & \\ K_1 - K_2^{-1} & I & \\ & & I \end{pmatrix}^{-1}$$

$$= \begin{pmatrix} 2I - K_2K_1 & K_2 & \\ -K_2^{-1} & 0 & \\ & & I \end{pmatrix}$$

$$= \begin{pmatrix} 2+ab & & & b & \\ & 2+ab & -b & & \\ & b^{-1} & 0 & & \\ -b^{-1} & & & 0 & \\ & & & & I \end{pmatrix} = L,$$

以及

$$\begin{pmatrix} 1 & & & & \\ & 0 & & c & \\ & & 1 & & \\ & c^{-1} & & 0 & \\ & & & & U \end{pmatrix} L \begin{pmatrix} 1 & & & & \\ & 0 & & c & \\ & & 1 & & \\ & c^{-1} & & 0 & \\ & & & & U \end{pmatrix}^{-1}$$

$$= \begin{pmatrix} \begin{pmatrix} 2+ab & bc^{-1} \\ -cb^{-1} & 0 \end{pmatrix} & & \\ & \begin{pmatrix} 0 & b^{-1}c \\ -c^{-1}b & 2+ab \end{pmatrix} & \\ & & I \end{pmatrix},$$

其中, 当 $\nu = 2$ 时, $c = -\frac{1}{2}(p\Delta p') \neq 0, U = I + 2(p\Delta p')\Delta p'p$; 而当 $\nu \geqslant 3$ 时, $c = 1$,

$$U = \begin{pmatrix} 0 & & 1 & & \\ & I & & & \\ 1 & & 0 & & \\ & & & I & \\ & & & & I \end{pmatrix}.$$

那么根据引理 2, $R^{-1}\mathfrak{N}R = \Omega_n(F,S)$. 所以 $\mathfrak{N} = \Omega_n(K,S)$.

(ii) M 的秩等于 1. 这时有可逆矩阵 A 和 B, 使

$$AMB' = \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix}.$$

于是

$$(1) \qquad \begin{pmatrix} A & \\ & B \end{pmatrix}\begin{pmatrix} P \\ PN \end{pmatrix} S \begin{pmatrix} P \\ PN \end{pmatrix}'\begin{pmatrix} A & \\ & B \end{pmatrix}' = \begin{pmatrix} 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 \\ 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \end{pmatrix},$$

因此 $\begin{pmatrix} P \\ PN \end{pmatrix}$ 的秩 $\geqslant 3$. 我们分别来讨论 $\begin{pmatrix} P \\ PN \end{pmatrix}$ 的秩等于 3 和 4 的情形:

(ii-1) $\begin{pmatrix} P \\ PN \end{pmatrix}$ 的秩等于 4. 这时 $\begin{pmatrix} P \\ PN \end{pmatrix}$ 含有一个 3 维的全迷向子空间, 因此 $\nu \geqslant 3$. 为了书写方便起见, 我们把 S 写成

$$S = \begin{pmatrix} 0 & I^{(3)} & \\ I^{(3)} & 0 & \\ & & S_1^{(n-6)} \end{pmatrix},$$

其中 S_1 是定号的, 如果 $\nu = 3$; 是不定号的, 如果 $\nu > 3$. 因为

$$\begin{pmatrix} 1 & 0 & 0 & 0 & 0 & 0 & 0^{(1,n-6)} \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 & 0 \end{pmatrix} S \begin{pmatrix} 1 & 0 & 0 & 0 & 0 & 0 & 0^{(1,n-6)} \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 & 0 \end{pmatrix}'$$

$$= \begin{pmatrix} 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 \\ 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \end{pmatrix},$$

所以根据定理 1.1, 有一个正交矩阵 R 存在, 使

$$\begin{pmatrix} 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 & 0 \end{pmatrix} = \begin{pmatrix} AP \\ BPN \end{pmatrix} R = \begin{pmatrix} APR \\ BPNR \end{pmatrix}.$$

像在情形 (i) 中一样计算, $R^{-1}\mathfrak{N}R$ 就含有

$$R^{-1}(T^{-1}N^{-1}TN)R = R^{-1}T^{-1}RR^{-1}(N^{-1}TN)R$$

$$=\begin{pmatrix}\begin{pmatrix}1 & & b\\ a & 1 & \\ & & 1\end{pmatrix} & & \\ & \begin{pmatrix}1 & -a & \\ & 1 & \\ -b & & 1\end{pmatrix} & \\ & & I\end{pmatrix}\quad (a=|A|^{-1}, b=|B|^{-1}).$$

于是, 根据引理 2, 就有 $R^{-1}\mathfrak{N}R=\Omega_n(F,S)$. 因此 $\mathfrak{N}=\Omega_n(F,S)$.

(ii-2) $\begin{pmatrix}P\\ PN\end{pmatrix}$ 的秩等于 3. 令 $B=\begin{pmatrix}\alpha & \beta\\ \gamma & \delta\end{pmatrix}$. 于是就有线性关系

$$(\lambda_1,\lambda_2)AP+\lambda_3(\alpha,\beta)PN+\lambda_4(\gamma,\delta)PN=0,$$

其中 $\lambda_1,\lambda_2,\lambda_3,\lambda_4$ 都是 F 里的元素, 而 λ_3 和 λ_4 不全为零. 从 (1) 式就可以推出 $\lambda_1=\lambda_3=0$, 因此不妨假定 $\lambda_4=1$, 即

$$(\gamma,\delta)PN=(0,\lambda_2)AP.$$

为了书写方便起见, 我们假定

$$S=\begin{pmatrix}0 & I^{(2)} & \\ I^{(2)} & 0 & \\ & & S_1^{(n-4)}\end{pmatrix},$$

而 S_1 是定号的, 如果 $\nu=2$; S_1 是不定号的, 如果 $\nu\geqslant 3$. 因为

$$\begin{pmatrix}1 & 0 & 0 & 0 & 0^{(1,n-4)}\\ 0 & 1 & 0 & 0 & 0\\ 0 & 0 & 1 & 0 & 0\end{pmatrix} S \begin{pmatrix}1 & 0 & 0 & 0 & 0^{(1,n-4)}\\ 0 & 1 & 0 & 0 & 0\\ 0 & 0 & 1 & 0 & 0\end{pmatrix}'=\begin{pmatrix}0 & 0 & 1\\ 0 & 0 & 0\\ 1 & 0 & 0\end{pmatrix},$$

所以根据定理 1.1, 就有一个正交矩阵 R, 使

$$\begin{pmatrix}1 & 0 & 0 & 0 & 0\\ 0 & 1 & 0 & 0 & 0\\ 0 & 0 & 1 & 0 & 0\end{pmatrix}=\begin{pmatrix}AP\\ (\alpha,\beta)PN\end{pmatrix}R.$$

那么

$$(\gamma,\delta)PNR=(0,\lambda_2)APR=(0,\lambda_2,0,0,0).$$

于是 $R^{-1}\mathfrak{N}R$ 就含有

$$\begin{aligned}R^{-1}(T^{-1}N^{-1}TN)R &= R^{-1}T^{-1}RR^{-1}(N^{-1}TN)R\\ &= \begin{pmatrix} \begin{pmatrix}1 & b\\ & 1\end{pmatrix} & & \\ \begin{pmatrix} & -a\\ a & ab\end{pmatrix} & \begin{pmatrix}1 & \\ -b & 1\end{pmatrix} & \\ & & I\end{pmatrix} = L \quad (a=|A^{-1}|, b=\lambda_2|B^{-1}|).\end{aligned}$$

又因为 $R^{-1}\mathfrak{N}R$ 也是 $\Omega_n(F,S)$ 的正规子群, 所以 $R^{-1}\mathfrak{N}R$ 也含有

$$L\begin{pmatrix}0 & 1 & & & \\ -1 & 0 & & & \\ & & 0 & 1 & \\ & & -1 & 0 & \\ & & & & I\end{pmatrix}L^{-1}\begin{pmatrix}0 & 1 & & & \\ -1 & 0 & & & \\ & & 0 & 1 & \\ & & -1 & 0 & \\ & & & & I\end{pmatrix}^{-1}$$

$$= \begin{pmatrix}\begin{pmatrix}1+b^2 & b\\ b & 1\end{pmatrix} & & \\ & \begin{pmatrix}1 & -b\\ -b & 1+b^2\end{pmatrix} & \\ & & I\end{pmatrix} = L_1$$

以及

$$\begin{pmatrix}\begin{pmatrix}1 & \\ -b^{-1} & 1\end{pmatrix} & & \\ & \begin{pmatrix}1 & b^{-1}\\ & 1\end{pmatrix} & \\ & & I\end{pmatrix} L_1 \begin{pmatrix}\begin{pmatrix}1 & \\ -b^{-1} & 1\end{pmatrix} & & \\ & \begin{pmatrix}1 & b^{-1}\\ & 1\end{pmatrix} & \\ & & I\end{pmatrix}^{-1}$$

$$K = \begin{pmatrix}\begin{pmatrix}2+b^2 & b\\ -b^{-1} & 0\end{pmatrix} & & \\ & \begin{pmatrix}0 & b^{-1}\\ -b & 2+b^2\end{pmatrix} & \\ & & I\end{pmatrix}.$$

根据引理 2, 就有 $R^{-1}\mathfrak{N}R = \Omega_n(F,S)$. 因此 $\mathfrak{N} = \Omega_n(F,S)$.

(iii) M 的秩等于 0. 这时,

$$\begin{pmatrix} P \\ PN \end{pmatrix} S \begin{pmatrix} P \\ PN \end{pmatrix}' = 0.$$

我们分别讨论 $\begin{pmatrix} P \\ PN \end{pmatrix}$ 的秩等于 4, 3 和 2 的情形.

(iii-1) $\begin{pmatrix} P \\ PN \end{pmatrix}$ 的秩等于 4. 这时 $\begin{pmatrix} P \\ PN \end{pmatrix}$ 是一个 4 维的全迷向子空间, 因此 $\nu \geqslant 4$. 为书写方便起见, 我们假定 $n=8$ 及 $\nu=4$. 因为

$$(I^{(4)}\ 0)S(I^{(4)}\ 0)' = 0^{(4)}.$$

所以就有正交矩阵 R, 使

$$(I^{(4)}\ 0) = \begin{pmatrix} P \\ PN \end{pmatrix} R.$$

因此 $R^{-1}\mathfrak{N}R$ 就含有

$$R^{-1}(T^{-1}N^{-1}TN)R = R^{-1}T^{-1}RR^{-1}(N^{-1}TN)R$$
$$= \begin{pmatrix} & I^{(4)} & & \\ \begin{pmatrix} & -1 \\ 1 & \end{pmatrix} & & & \\ & & \begin{pmatrix} & 1 \\ -1 & \end{pmatrix} & I^{(4)} \end{pmatrix} = L.$$

又因为 $R^{-1}\mathfrak{N}R$ 也是 $\Omega_n(F,S)$ 的正规子群, 所以 $R^{-1}\mathfrak{N}R$ 也含有

$$L\begin{pmatrix} I^{(2)} & \begin{matrix} 1 & 0 \\ 0 & 0 \end{matrix} & & \\ & I^{(2)} & & \\ & & I^{(2)} & \\ & & \begin{matrix} -1 & 0 \\ 0 & 0 \end{matrix} & I^{(2)} \end{pmatrix} L^{-1} \begin{pmatrix} I^{(2)} & \begin{matrix} 1 & 0 \\ 0 & 0 \end{matrix} & & \\ & I^{(2)} & & \\ & & I^{(2)} & \\ & & \begin{matrix} -1 & 0 \\ 0 & 0 \end{matrix} & I^{(2)} \end{pmatrix}^{-1}$$
$$= \begin{pmatrix} I^{(4)} & & \begin{matrix} & 0 \\ 1 & \end{matrix} & \\ \begin{matrix} & -1 \\ 0 & \end{matrix} & & I^{(4)} \end{pmatrix},$$

这是一个 2 平延. 因此根据引理 1, 就有 $R^{-1}\mathfrak{N}R = \Omega_n(F,S)$. 所以 $\mathfrak{N} = \Omega_n(F,S)$.

(iii-2) $\begin{pmatrix} P \\ PN \end{pmatrix}$ 的秩等于 3. 这时 $\begin{pmatrix} P \\ PN \end{pmatrix}$ 是 3 维的全迷向子空间, 因此 $\nu \geqslant 3$. 为书写方便起见, 我们假定 $n=6, \nu=3$. 令 $P = \begin{pmatrix} v_1 \\ v_2 \end{pmatrix}$. 我们不妨假定 $\begin{pmatrix} v_1 \\ v_2 \\ v_1 N \end{pmatrix}$ 的秩等于 3. 那么

$$v_2 N = \lambda_1 v_1 + \lambda_2 v_2 + \lambda_3 v_1 N,$$

因为

$$(I^{(3)}\ 0^{(3)})S(I^{(3)}\ 0^{(3)})' = 0^{(3)},$$

所以就有一个正交矩阵 R, 使

$$(I^{(3)}\ 0^{(3)}) = \begin{pmatrix} v_1 \\ v_2 \\ v_1 N \end{pmatrix} R,$$

因而

$$v_2 NR = (\lambda_1, \lambda_2, \lambda_3, 0, 0, 0).$$

于是 $R^{-1}\mathfrak{N}R$ 就含有

$$R^{-1}(T^{-1}N^{-1}TN)R = \begin{pmatrix} I^{(3)} & \\ \begin{pmatrix} 0 & -1 & -\lambda_1 \\ 1 & 0 & -\lambda_2 \\ \lambda_1 & \lambda_2 & 0 \end{pmatrix} & I^{(3)} \end{pmatrix},$$

这是一个 2 平延. 因此, 根据引理 1, 就有 $R^{-1}\mathfrak{N}R = \Omega_n(F,S)$. 所以 $\mathfrak{N} = \Omega_n(F,S)$.

(iii-3) $\begin{pmatrix} P \\ PN \end{pmatrix}$ 的秩等于 2. 这时 $PN = QP$, Q 是个 2 行 2 列的可逆矩阵, 同时 $\nu \geqslant 2$. 为书写方便起见, 我们假定把 S 写成

$$S = \begin{pmatrix} 0 & I^{(2)} & \\ I^{(2)} & 0 & \\ & & S_1 \end{pmatrix}.$$

因为

$$(I^{(2)}, 0^{(2)}, 0^{(2,n-4)})S(I^{(2)}, 0^{(2)}, 0^{(2,n-4)})' = 0,$$

所以就有正交矩阵 R, 使

$$(I^{(2)}, 0^{(2)}, 0^{(2,n-4)}) = PR.$$

因此

$$PNR = QPR = Q(I^{(2)}\ 0\ 0).$$

那么 $R^{-1}\mathfrak{N}R$ 就含有

$$R^{-1}(T^{-1}N^{-1}TN)R = \begin{pmatrix} & I & & \\ \begin{pmatrix} 0 & a-1 \\ 1-a & 0 \end{pmatrix} & & I & \\ & & & I \end{pmatrix},$$

其中 $a = |Q|$. 因为 $T^{-1}N^{-1}TN \neq I$, 所以 $R^{-1}(T^{-1}N^{-1}TR)R$ 是个 2 平延. 因此根据引理 1, 就有 $R^{-1}\mathfrak{N}R = \Omega_n(F,S)$. 所以 $\mathfrak{N} = \Omega_n(F,S)$.

至此, 我们的定理就完全证明了.

第十章　特征数为 2 的域上的二次型和无亏数的正交群

§1　二次型的合同及 Witt 定理的推广

设 F 是特征数为 2 的域. 考查 F 上所有 $n \times n$ 矩阵的集合 M_n, 它对于矩阵加法组成一群. 以 K_n 表 M_n 中所有交错矩阵所组成的子群. 我们有商群 M_n/K_n. 我们说 M_n 中两个元素 A 和 B 同余 mod K_n, 如果 $A + B \in K_n$, 这时我们写 $A \equiv B \pmod{K_n}$. 易见, M_n 中的元素同余 mod K_n 这个关系是个等价关系.

对于每个 $A \in M_n$, 令一个 n 元二次型

$$(x_1, \cdots, x_n)A(x_1, \cdots, x_n)'$$

与之相应. 易见, 两个矩阵 $A, B \in M_n$ 给出同一 n 元二次型, 当且仅当 $A \equiv B \pmod{K_n}$. 反之, 一个 n 元二次型

$$\sum_{1 \leqslant i \leqslant j \leqslant n} a_{ij} x_i x_j$$

可表成

$$(x_1, \cdots, x_n) \begin{pmatrix} b_{11} & \cdots & b_{1n} \\ \cdots & \cdots & \cdots \\ b_{n1} & \cdots & b_{nn} \end{pmatrix} \begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix},$$

其中 $b_{ii} = a_{ii}, b_{ij} + b_{ji} = a_{ij}$ 如 $i < j$. 矩阵 $B = (b_{ij})$ 除差一 K_n 中矩阵外, 是唯一确定的. 这样我们就在 n 元二次型和 M_n/K_n 中的元素之间, 或 M_n 的 mod K_n 同余的矩阵类之间建立了一个一一对应.

我们的目的是研究二次型的合同, 为此给出

定义 1　两个同余矩阵类 $\mathfrak{A}$ 和 $\mathfrak{B}$ 称为合同, 如果有可逆矩阵 C 存在, 使

$$CAC' \equiv B \pmod{K_n},$$

而 $A \in \mathfrak{A}, B \in \mathfrak{B}$. 称两个二次型合同, 如果相应的矩阵类合同.

易证这个定义与 A 和 B 的特殊选取无关. 实际上, 如 K 交错, 则 CKC' 亦然.

定理 1　任一同余矩阵类皆与含形为

$$(1)\qquad \begin{pmatrix} A & I & 0 & 0 \\ 0 & B & 0 & 0 \\ 0 & 0 & C & 0 \\ 0 & 0 & 0 & 0 \end{pmatrix}$$

的一个矩阵的同余矩阵类合同, 其中 $A=[\alpha_1,\cdots,\alpha_p], B=[\beta_1,\cdots,\beta_p]$ 及 $C=[\gamma_1,\cdots,\gamma_{n-2p-q}]$ 皆为对角阵, 而 $\sum_{i=2p+1}^{n-q}\gamma_{i-2p}x_i^2=0$ 推出

$$x_{2p+1}=x_{2p+2}=\cdots=x_{n-q}=0.$$

换言之, 任一二次型皆合同于形为

$$(2)\qquad \sum_{i=1}^{q}(\alpha_i x_i^2+x_i x_{p+i}+\beta_i x_{p+i}^2)+\sum_{i=2p+1}^{n-q}\gamma_{i-2p}x_i^2$$

的一个二次型, 而 $\sum_{i=2p+1}^{n-q}\gamma_{i-2p}x_i^2=0$ 推出 $x_{2p+1}=x_{2p+2}=\cdots=x_{n-q}=0$. 更进一步, p 和 $n-2p-q$ 这两个数唯一确定.

【证】 不妨设所给的同余矩阵类中含一三角形矩阵 P. 如 P 有一非对角元素 $\neq 0$, 不妨设 $a_{12}\neq 0$. 写

$$P=\begin{pmatrix} a_{11} & a_{12} & \\ 0 & a_{22} & L \\ & 0 & Q \end{pmatrix},$$

于是

$$\begin{pmatrix} I & 0 \\ L'\begin{pmatrix} 0 & a_{12}^{-1} \\ a_{12}^{-1} & 0 \end{pmatrix} & I \end{pmatrix}\begin{pmatrix} a_{11} & a_{12} & \\ 0 & a_{22} & L \\ & 0 & Q \end{pmatrix}$$

$$\cdot\begin{pmatrix} I & 0 \\ L'\begin{pmatrix} 0 & a_{12}^{-1} \\ a_{12}^{-1} & 0 \end{pmatrix} & I \end{pmatrix}'\equiv\begin{pmatrix} a_{11} & a_{12} & \\ 0 & a_{22} & 0 \\ & 0 & P_1 \end{pmatrix},$$

而

$$P_1=L'\begin{pmatrix} 0 & a_{12}^{-1} \\ a_{12}^{-1} & 0 \end{pmatrix}\begin{pmatrix} a_{11} & a_{12} \\ 0 & a_{22} \end{pmatrix}\begin{pmatrix} 0 & a_{12}^{-1} \\ a_{12}^{-1} & 0 \end{pmatrix}L+Q.$$

因

$$\begin{pmatrix} 1 & 0 \\ 0 & a_{12}^{-1} \end{pmatrix}\begin{pmatrix} a_{11} & a_{12} \\ 0 & a_{22} \end{pmatrix}\begin{pmatrix} 1 & 0 \\ 0 & a_{12}^{-1} \end{pmatrix}=\begin{pmatrix} a_{11} & 1 \\ 0 & a_{12}^{-2}a_{22} \end{pmatrix},$$

故 P 的类合同于一类含有

$$\begin{pmatrix} \begin{matrix}\alpha_1 & 1 \\ 0 & \beta_1\end{matrix} & 0 \\ 0 & P_1 \end{pmatrix},$$

而 $\alpha_1 = a_{11}, \beta_1 = a_{12}^{-2}a_{22}$. 依归纳法假设, P 的类合同于一类含有

$$\begin{pmatrix}
\alpha_1 & 1 & & & & & & & & & \\
0 & \beta_1 & & & & & & & & & \\
 & & \alpha_2 & & & 1 & & & & & \\
 & & & \ddots & & & \ddots & & & & \\
 & & & & \alpha_p & & & 1 & & & \\
 & & & & & \beta_2 & & & & & \\
 & & & & & & \ddots & & & & \\
 & & & & & & & \beta_p & & & \\
 & & & & & & & & \gamma_1 & & \\
 & & & & & & & & & \ddots & \\
 & & & & & & & & & & \gamma_r \\
 & & & & & & & & & & & 0
\end{pmatrix},$$

因而合同于一类含有

$$\begin{pmatrix} A & I & 0 & 0 \\ 0 & B & 0 & 0 \\ 0 & 0 & C & 0 \\ 0 & 0 & 0 & 0 \end{pmatrix},$$

其中 $A = [\alpha_1, \cdots, \alpha_p], B = [\beta_1, \cdots, \beta_p], C = [\gamma_1, \cdots, \gamma_r]$. 如 $\sum_{i=1}^{r} \gamma_i x_{2p+i}^2 = 0$ 而 $x_{2p+1}, x_{2p+2}, \cdots, x_{2p+r}$ 不全为 0, 可设 $x_{2p+r} \neq 0$, 于是

$$\begin{pmatrix}
1 & & & & \\
 & 1 & & & \\
 & & \ddots & & \\
 & & & 1 & \\
x_{2p+r}^{-1}x_{2p+1} & x_{2p+r}^{-1}x_{2p+2} & \cdots & x_{2p+r}^{-1}x_{2p+r-1} & 1
\end{pmatrix}
\begin{pmatrix}
\gamma_1 & & & & \\
 & \gamma_2 & & & \\
 & & \ddots & & \\
 & & & \ddots & \\
 & & & & \gamma_r
\end{pmatrix}$$

$$\cdot\begin{pmatrix} 1 & & & & \\ & 1 & & & \\ & & \ddots & & \\ & & & 1 & \\ x_{2p+r}^{-1}x_{2p+1} & x_{2p+r}^{-1}x_{2p+2} & \cdots & x_{2p+r}^{-1}x_{2p+r-1} & 1 \end{pmatrix}' = \begin{pmatrix} \gamma_1 & & & & \\ & \gamma_2 & & & \\ & & \ddots & & \\ & & & \gamma_{r-1} & \\ & & & & 0 \end{pmatrix},$$

如此进行下去, 即可将 P 化为 (1).

如 P 中非对角元素皆 0, 按照以上证明中的最后一步即可将 P 化为 (1). 但需注意, 这时 (1) 中 $p=0$.

最后, 设

$$\begin{pmatrix} A & I & 0 & 0 \\ 0 & B & 0 & 0 \\ 0 & 0 & C & 0 \\ 0 & 0 & 0 & 0 \end{pmatrix} \text{和} \begin{pmatrix} A_1 & I_1 & 0 & 0 \\ 0 & B_1 & 0 & 0 \\ 0 & 0 & C_1 & 0 \\ 0 & 0 & 0 & 0 \end{pmatrix}$$

合同, $A_1=[\alpha_1',\cdots,\alpha_{p_1}'], B_1=[\beta_1',\cdots,\beta_{p_1}'], C_1=[\gamma_1',\cdots,\gamma_{n-2p_1-q_1}']$. 于是有可逆矩阵 D 存在, 使

$$D\begin{pmatrix} A & I & 0 & 0 \\ 0 & B & 0 & 0 \\ 0 & 0 & C & 0 \\ 0 & 0 & 0 & 0 \end{pmatrix}D' \equiv \begin{pmatrix} A_1 & I_1 & 0 & 0 \\ 0 & B_1 & 0 & 0 \\ 0 & 0 & C_1 & 0 \\ 0 & 0 & 0 & 0 \end{pmatrix}.$$

因之

$$D\left[\begin{pmatrix} A & I & & \\ & B & & \\ & & C & \\ & & & 0 \end{pmatrix} + \begin{pmatrix} A & I & & \\ & B & & \\ & & C & \\ & & & 0 \end{pmatrix}'\right]D'$$

$$= \begin{pmatrix} A_1 & I_1 & & \\ & B_1 & & \\ & & C_1 & \\ & & & 0 \end{pmatrix} + \begin{pmatrix} A_1 & I_1 & & \\ & B_1 & & \\ & & C_1 & \\ & & & 0 \end{pmatrix}',$$

即

$$D\begin{pmatrix} 0 & I & \\ I & 0 & \\ & & 0 \end{pmatrix}D' = \begin{pmatrix} 0 & I_1 & \\ I_1 & 0 & \\ & & 0 \end{pmatrix}.$$

由是 $p = p_1$.

写

$$P = \begin{pmatrix} A & I \\ 0 & B \end{pmatrix}, \quad P_1 = \begin{pmatrix} A_1 & I \\ 0 & B_1 \end{pmatrix}$$

及

$$D = \begin{pmatrix} D_{11}^{(2p)} & D_{12} \\ D_{21} & D_{22} \end{pmatrix},$$

则从

$$(3) \qquad \begin{pmatrix} D_{11} & D_{12} \\ D_{21} & D_{22} \end{pmatrix} \begin{pmatrix} P & & \\ & C & \\ & & 0 \end{pmatrix} \begin{pmatrix} D_{11} & D_{12} \\ D_{21} & D_{22} \end{pmatrix}' \equiv \begin{pmatrix} P_1 & & \\ & C_1 & \\ & & 0 \end{pmatrix}$$

推出

$$\begin{pmatrix} D_{11} & D_{12} \\ D_{21} & D_{22} \end{pmatrix} \begin{pmatrix} 0 & I^{(p)} & \\ I & 0 & \\ & & 0 \end{pmatrix} \begin{pmatrix} D_{11} & D_{12} \\ D_{21} & D_{22} \end{pmatrix}' = \begin{pmatrix} 0 & I^{(p)} & \\ I & 0 & \\ & & 0 \end{pmatrix}.$$

写

$$K = \begin{pmatrix} 0 & I^{(p)} \\ I & 0 \end{pmatrix},$$

则有

$$D_{21}K(D_{11}'D_{21}') = (0, 0).$$

由此推出 $D_{21} = 0$. 再从 (3) 推出

$$D_{22} \begin{pmatrix} C & 0 \\ 0 & 0 \end{pmatrix} D_{22}' \equiv \begin{pmatrix} C_1 & 0 \\ 0 & 0 \end{pmatrix}.$$

利用性质 $\sum_{i=2p+1}^{n-q} \gamma_{i-2p} x_i^2 = 0$ 推出 $x_{2p+1} = \cdots = x_{n-q} = 0$ 及 $\sum_{i=2p+1}^{n-q_1} \gamma_{i-2p}' x_i^2 = 0$ 推出 $x_{2p+1} = \cdots = x_{n-q_1} = 0$ 可得 $q = q_1$.

定义 2　n 元二次型称为正则, 如它合同于形如 (2) 的一个二次型而其中 $q = 0$. 相应于正则 n 元二次型的矩阵也称为正则.

以下我们只限于研究正则二次型.

定义 3　n 元正则二次型中 $d = n - 2p$ 这个数称为它的亏数, 而二次型称为是具亏数 d 的. 如 $d = 0$, 则二次型称为是无亏数的.

如一 n 元正则二次型由矩阵 P 表出, 则易证它的亏数等于 $n - (P + P')$ 的秩.

为了进一步研究正则二次型的合同, 所谓 Witt 定理实属基本. 先研究以下特例.

定理 2 设

$$\begin{pmatrix} 0 & 1 & \\ 0 & 0 & \\ & & B \end{pmatrix} \text{和} \begin{pmatrix} 0 & 1 & \\ 0 & 0 & \\ & & B_1 \end{pmatrix}$$

是合同的正则矩阵, 则 B 与 B_1 也合同.

【证】 写 $A=\begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix}$. 依假设有可逆矩阵

$$\begin{pmatrix} P & Q \\ S & T \end{pmatrix}$$

存在, 使

$$\begin{pmatrix} P & Q \\ S & T \end{pmatrix}\begin{pmatrix} A & 0 \\ 0 & B \end{pmatrix}\begin{pmatrix} P' & S' \\ Q' & T' \end{pmatrix} \equiv \begin{pmatrix} A & 0 \\ 0 & B_1 \end{pmatrix},$$

即

$$\begin{aligned} &PAP' + QBQ' \equiv A, \\ &PAS' + QBT' + (SAP' + TBQ')' = 0, \\ &SAS' + TBT' \equiv B_1. \end{aligned}$$

上面的第二个关系式可改写作

$$P(A+A')S' + Q(B+B')T' = 0.$$

于是, 如 $I+P$ 可逆, 则有

$$(S(I+P)^{-1}Q+T)B(S(I+P)^{-1}Q+T)' \equiv B_1.$$

因 B 和 B_1 是正则矩阵, $S(I+P)^{-1}Q+T$ 可逆, 这时定理成立. 如 $I+P$ 不可逆, 考查

$$(SXQ+T)B(SXQ+T)',$$

而 X 待定. 我们有

$$\begin{aligned} &(SXQ+T)B(SXQ+T)' \\ \equiv &S[XPAP'X' + XAX' + XPA + XPA']S' + TBT'. \end{aligned}$$

如 $P=I$, 取 $X=\begin{pmatrix}1&0\\0&0\end{pmatrix}$, 就有

$$(SXQ+T)B(SXQ+T)'=SAS'+TBT'\equiv B_1.$$

如 $P\neq I$, 可设

(4) $$P=\begin{pmatrix}1&0\\c&d\end{pmatrix}\text{或}\begin{pmatrix}1&1\\0&0\end{pmatrix}.$$

实际上,

$$\begin{pmatrix}U&\\&I\end{pmatrix}\begin{pmatrix}P&Q\\S&T\end{pmatrix}\begin{pmatrix}V&\\&I\end{pmatrix}\begin{pmatrix}V^{-1}&\\&I\end{pmatrix}\begin{pmatrix}A&\\&B\end{pmatrix}\begin{pmatrix}V^{-1}&\\&I\end{pmatrix}'$$
$$\cdot\begin{pmatrix}V&\\&I\end{pmatrix}'\begin{pmatrix}P&Q\\S&T\end{pmatrix}'\begin{pmatrix}U&\\&I\end{pmatrix}'\equiv\begin{pmatrix}U&\\&I\end{pmatrix}\begin{pmatrix}A&\\&B_1\end{pmatrix}\begin{pmatrix}U&\\&I\end{pmatrix}'.$$

于是, 如 $UAU'\equiv A$ 及 $V^{-1}AV^{-1'}\equiv A$, 则

$$\begin{pmatrix}UPV&UQ\\SV&T\end{pmatrix}\begin{pmatrix}A&\\&B\end{pmatrix}\begin{pmatrix}UPV&UQ\\SV&T\end{pmatrix}'=\begin{pmatrix}A&\\&B_1\end{pmatrix}.$$

写 $P=\begin{pmatrix}a&b\\c&d\end{pmatrix}$. 因 $P+I$ 不可逆, P 中有一非零元. 又因

$$\begin{pmatrix}0&1\\1&0\end{pmatrix}A\begin{pmatrix}0&1\\1&0\end{pmatrix}\equiv A,$$

可设 $a\neq 0$. 于是

$$\begin{pmatrix}a^{-1}&0\\0&a\end{pmatrix}\begin{pmatrix}a&b\\c&d\end{pmatrix}=\begin{pmatrix}1&a^{-1}b\\ac&ad\end{pmatrix}.$$

因此可设 $a=1$. 那么, $P=\begin{pmatrix}1&b\\c&d\end{pmatrix}$. 从 $|P+I|=0$ 推出 $bc=0$. 如 $b=0, P=\begin{pmatrix}1&0\\c&d\end{pmatrix}$. 如 $b\neq 0$, 则 $c=0$. 如 $d\neq 0$, 则有

$$\begin{pmatrix}0&1\\1&0\end{pmatrix}\begin{pmatrix}1&b\\0&d\end{pmatrix}\begin{pmatrix}0&1\\1&0\end{pmatrix}=\begin{pmatrix}0&d\\1&b\end{pmatrix}\begin{pmatrix}0&1\\1&0\end{pmatrix}=\begin{pmatrix}d&0\\b&1\end{pmatrix},$$

$$\begin{pmatrix}d^{-1}&\\&d\end{pmatrix}\begin{pmatrix}d&0\\b&1\end{pmatrix}=\begin{pmatrix}1&0\\db&1\end{pmatrix}.$$

如 $d=0$, 则

$$\begin{pmatrix} 1 & b \\ 0 & 0 \end{pmatrix}\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}=\begin{pmatrix} b & 1 \\ 0 & 0 \end{pmatrix}.$$

如 $b\neq 1$, 则 $\left|\begin{pmatrix} b & 1 \\ 0 & 0 \end{pmatrix}+I\right|\neq 0$, 这就化到前一情形. 因此 $b=1$. 这样我们总有 (4). 这时我们也取 $X=\begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix}$, 则

$$(SXQ+T)B(SXQ+T)'=B_1.$$

定理就完全证明了.

定理 3 设 A 是无亏数的正则矩阵, 则

$$\begin{pmatrix} A & 0 \\ 0 & A \end{pmatrix}$$

合同于

$$\begin{pmatrix} 0 & I \\ 0 & 0 \end{pmatrix}.$$

证 只需证

$$\begin{pmatrix} \alpha & 1 & & \\ & \beta & & \\ & & \alpha & 1 \\ & & & \beta \end{pmatrix}$$

与

$$\begin{pmatrix} 0 & I^{(2)} \\ & 0 \end{pmatrix}$$

合同. 我们有

$$\begin{pmatrix} I & I \\ & I \end{pmatrix}\begin{pmatrix} \alpha & 1 & & \\ & \beta & & \\ & & \alpha & 1 \\ & & & \beta \end{pmatrix}\begin{pmatrix} I & \\ I & I \end{pmatrix}\equiv\begin{pmatrix} 0 & & 0 & 1 \\ & & 1 & 0 \\ & & \alpha & 1 \\ & & & \beta \end{pmatrix},$$

$$\begin{pmatrix} 0 & 1 & \\ 1 & 0 & \\ & & I \end{pmatrix}\begin{pmatrix} 0 & & 0 & 1 \\ & & 1 & 0 \\ & & \alpha & 1 \\ & & & \beta \end{pmatrix}\begin{pmatrix} 0 & 1 & \\ 1 & 0 & \\ & & I \end{pmatrix}=\begin{pmatrix} 0 & & I & \\ & \alpha & & 1 \\ 0 & & & \\ & & & \beta \end{pmatrix},$$

$$\begin{pmatrix} & I & \\ \alpha & 1 & \\ & & I \\ & \beta & \end{pmatrix}\begin{pmatrix} 0 & & I \\ & \alpha & 1 \\ 0 & & \\ & & \beta \end{pmatrix}\begin{pmatrix} & \alpha & 1 \\ I & & \\ & & \beta \\ & I & \end{pmatrix} = \begin{pmatrix} 0 & I \\ 0 & 0 \end{pmatrix}.$$

定理 4　(Witt 定理的推广)　设

$$\begin{pmatrix} A & \\ & B \end{pmatrix} \text{ 和 } \begin{pmatrix} A & \\ & B_1 \end{pmatrix}$$

是合同的正则矩阵, 而 A 是无亏数的, 则 B 和 B_1 亦合同.

证　从

$$\begin{pmatrix} A & 0 \\ 0 & B \end{pmatrix} \text{ 和 } \begin{pmatrix} A & 0 \\ 0 & B_1 \end{pmatrix}$$

合同, 推出

$$\begin{pmatrix} A & & \\ & A & \\ & & B \end{pmatrix} \text{ 和 } \begin{pmatrix} A & & \\ & A & \\ & & B_1 \end{pmatrix}$$

合同. 依定理 3,

$$\begin{pmatrix} 0 & I & \\ 0 & 0 & \\ & & B \end{pmatrix} \text{和} \begin{pmatrix} 0 & I & \\ 0 & 0 & \\ & & B_1 \end{pmatrix}$$

合同, 最后再由定理 2 推出 B 和 B_1 合同.

§2　奇异子空间　正则二次型的指数

设 $g(x_1, \cdots, x_n) = \sum\limits_{1 \leqslant i \leqslant j \leqslant n} a_{ij}x_ix_j$ 是个正则二次型. 设 G 是一个表 $g(x_1, \cdots, x_n)$ 的矩阵, 则 $G + G'$ 是交错矩阵, 而且这个交错矩阵是与 G 的选取无关的. 我们可以研究对于 $G + G'$ 的迷向向量, 迷向子空间及全迷向子空间等. 像以前一样, 以 V^* 表 V 的共轭子空间.

定义 1　设 $g(x_1, \cdots, x_n)$ 是个 n 元正则二次型. 一向量 $(a_1, \cdots, a_n)$ 称为奇异, 如 $g(a_1, \cdots, a_n) = 0$; 否则它称为非奇异. 一个子空间 V 称为奇异, 如果 $V \cap V^*$

中含一个非零子空间, 使得 $g(a_1,\cdots,a_n)=0$, 对这个非零子空间中任一向量; 否则, V 称为非奇异的. V 称为全奇异的, 如 $g(a_1,\cdots,a_n)=0$, 对所有 $(a_1,\cdots,a_n)\in V$.

定理 1 设 $g(x_1,\cdots,x_n)$ 是 n 元正则二次型, 而 G 是表 $g(x_1,\cdots,x_n)$ 的矩阵, 则对于 g 的奇异向量, 奇异子空间和全奇异子空间分别是对于 $G+G'$ 的迷向向量, 迷向子空间和全迷向子空间.

【证】 对于奇异向量, 奇异子空间定理显然成立. 现在设 V 是全奇异子空间. 设 $v_1,v_2\in V$, 则 $v_1Gv_1'=0$ 和 $v_2Gv_2'=0$, 及

$$(v_1+v_2)G(v_1+v_2)'=0,$$

于是

$$\begin{aligned}0=&(v_1+v_2)G(v_1+v_2)'\\=&v_1Gv_1'+v_1Gv_2'+v_2Gv_1'+v_2Gv_2'\\=&v_1(G+G')v_2'.\end{aligned}$$

这就证明了 V 是全迷向的.

从定义 1 及定理 1 立刻推出: 向量 $(a_1,\cdots,a_n)$ 是奇异的, 当且仅当 $(a_1,\cdots,a_n)G(a_1,\cdots,a_n)'=0$. 线性子空间 V 奇异, 当且仅当矩阵 VGV' 奇异. V 全奇异当且仅当 $VGV'\equiv 0$.

定理 2 一非迷向的平面包含 0 条或 2 条奇异直线. 一个迷向的但不是全奇异的平面包含 0 条或 1 条奇异直线.

【证】 这是以下关系式的直接推论:

$(\lambda v_1+v_2)G(\lambda v_1+v_2)'=\lambda^2v_1Gv_1'+\lambda v_1(G+G')v_2'+v_2Gv_2'.$

定义 2 设 $g(x_1,\cdots,x_n)$ 是个正则二次型, 它的全奇异子空间的最大维数称为它的指数, 正则矩阵的指数就定义为它所表示的正则二次型的指数.

易见, 正则二次型的指数在合同之下不变.

定理 3 任一指数为 ν 的正则矩阵 G 皆合同于

$$\begin{pmatrix}0 & I^{(\nu)} & \\ 0 & 0 & \\ & & G_1\end{pmatrix}, \tag{5}$$

其中 $(x_{2\nu+1},\cdots,x_n)G_1(x_{2\nu+1},\cdots,x_n)'=0$ 推出 $x_{2\nu+1}=\cdots=x_n=0$.

【证】 设 X 是个极大维 ν 的全奇异子空间. 设 Y 是个 $n-\nu$ 维的线性子空间, 使

$$\begin{pmatrix}X\\Y\end{pmatrix}$$

可逆, 于是

$$\begin{pmatrix} X \\ Y \end{pmatrix} G \begin{pmatrix} X \\ Y \end{pmatrix}'$$
$$= \begin{pmatrix} 0 & XGY' \\ YGX' & YGY' \end{pmatrix} \equiv \begin{pmatrix} 0 & X(G+G')Y' \\ & YGY' \end{pmatrix}.$$

因 G 正则, $X(G+G')Y'$ 的秩为 ν, 于是 $n \geqslant 2\nu$. 有可逆矩阵 P 和 Q 存在, 使

$$PX(G+G')Y'Q' = (I^{(\nu)}\ 0).$$

于是

$$\begin{pmatrix} P & \\ & Q \end{pmatrix} \begin{pmatrix} 0 & X(G+G')Y' \\ 0 & YGY' \end{pmatrix} \begin{pmatrix} P' & \\ & Q' \end{pmatrix} = \begin{pmatrix} 0 & I^{(\nu)} & 0 \\ 0 & A & B \\ 0 & 0 & D \end{pmatrix}.$$

那么

$$\begin{pmatrix} I & & \\ A & I & \\ B' & & I \end{pmatrix} \begin{pmatrix} 0 & I & \\ & A & B \\ & & 0 \end{pmatrix} \begin{pmatrix} I & A' & B \\ & I & \\ & & I \end{pmatrix} \equiv \begin{pmatrix} 0 & I & 0 \\ 0 & 0 & 0 \\ 0 & 0 & D \end{pmatrix}.$$

因 G 的指数为 ν, 故 $(x_{2\nu+1},\cdots,x_n)D(x_{2\nu+1},\cdots,x_n)'=0$ 推出

$$x_{2\nu+1}=\cdots=x_n=0.$$

定理 4 极大全奇异子空间的维数一定相等, 即等于 G 的指数 ν.

【证】 设 P 是个极大全奇异子空间, 维数为 d, 则依定理 3 的证明, G 合同于

$$\begin{pmatrix} 0 & I^{(d)} & \\ & 0 & \\ & & D_1 \end{pmatrix}, \tag{6}$$

因 P 是极大全奇异子空间, $(x_{2d+1},\cdots,x_n)D_1(x_{2d+1},\cdots,x_n)'=0$ 推出 $x_{2d+1}=\cdots=x_n=0$. 由 (5), (6) 合同及 Witt 定理推出

$$\begin{pmatrix} 0 & I^{(\nu-d)} & \\ & 0 & \\ & & G_1 \end{pmatrix} \text{ 与 } D_1$$

合同. 这与性质 $(x_{2d+1},\cdots,x_n)D(x_{2d+1},\cdots,x_n)'=0$ 推出 $x_{2d+1}=\cdots=x_n=0$ 抵触, 除非 $\nu=d$.

§3 正 交 群

设 G 是 $n\times n$ 正则矩阵. 一切 $n\times n$ 矩阵 T 适合条件

$$TGT'\equiv G \pmod{K_n}$$

者组成一群, 而且这个群仅与 G 所属的 M_n/K_n 的陪集有关而与 G 的特殊选取无关. 这个群称为 F 上对于 G 的 n 级正交群, 记作 $O_n(F,G)$. $O_n(F,G)$ 的换位子群记作 $\Omega_n(F,G)$.

如 G 和 H 是合同的正则矩阵, 即有可逆的 C 存在, 使

$$CGC'\equiv H \pmod{K_n},$$

则在对应

$$T\to CTC^{-1}$$

之下, $O_n(F,G)$ 与 $O_n(F,H)$ 同构. 因此为研究正交群的构造, 不妨设

$$G=\begin{pmatrix} 0 & I^{(\nu)} & & & \\ 0 & 0 & & & \\ & & A & I & \\ & & 0 & B & \\ & & & & C \end{pmatrix}$$

其中 $A=[\alpha_1\cdots,\alpha_{p-\nu}],B=[\beta_1,\cdots,\beta_{p-\nu}],C=[\gamma_1,\cdots,\gamma_{n-2p}]$ 是对角阵, 而

$$\begin{pmatrix} A & I & \\ & B & \\ & & C \end{pmatrix}$$

的指数为 0.

在本章中, 我们先研究无亏数的 G 所定义的正交群, 而不再作声明. 我们取

$$G=\begin{pmatrix} 0 & I^{(\nu)} & & \\ 0 & 0 & & \\ & & A & I \\ & & 0 & B \end{pmatrix}.$$

关于这一情形的正交群 $O_n(F,G)$ 的研究与特征数 $\neq 2$ 的域 F 上正交群 $O_n(F,S)$ 的研究完全平行, 因此, 我们在以下只扼要地讨论一下群 $O_n(F,G)$, 而将重点放在不同之处.

首先, 我们指出, 从 $TGT' \equiv G$ 推出 $T(G+G')T' = G+G'$. 这就是说, 如 $T \in O_n(F,G)$, 则 $T \in Sp_n(F, G+G')$. 因此, $O_n(F,G)$ 是 $Sp_n(F,G+G')$ 的子群. 以下令 $S = G+G'$.

定义 1 同一维数的两个子空间 V_1 和 V_2 称为正交等价, 如有一可逆矩阵 P 和一正交矩阵 T 存在, 使

$$V_1 = PV_2T$$

(参看第七章定义 6.1).

定理 1 设 V_1 和 V_2 是两个同一维数的非迷向子空间, 则 V_1 和 V_2 正交等价当且仅当 V_1GV_1' 和 V_2GV_2' 合同.

可仿第七章定理 6.1 证之.

系理 1 设 V_1 和 V_2 是两个同一维数的非迷向子空间. 如果 $V_1GV_1' \equiv V_2GV_2'$, 则有 $T \in O_n(F,G)$, 使 $V_1T = V_2$.

参看第七章定理 6.1 的系理 2.

定理 2 设 V_1 和 V_2 是同一维数的两个全奇异子空间, 则 V_1 和 V_2 正交等价, 更进一步, 我们有 $V_1 = V_2T$.

亦可仿第七章定理 6.1 证之.

定理 3 设 v_1 和 v_2 是两个非奇异向量, 则 v_1 和 v_2 正交等价当且仅当 v_1Gv_1' 和 v_2Gv_2' 合同.

【证】 如 v_1 和 v_2 正交等价, 自然 v_1Gv_1' 和 v_2Gv_2' 合同. 反之, 设 v_1Gv_1' 和 $v_2Gv'_2$ 合同. 设

$$v_1Gv_1' = a^2v_2Gv_2'.$$

先研究 $\nu = 0$ 的情形. 如 $v_1Sv_2' = 0$, 则

$$(v_1+av_2)G(v_1+av_2)' = 0,$$

于是 $v_1 = av_2$. 这时 v_1 自然与 v_2 正交等价. 让我们假设 $v_1Sv_2' \neq 0$. 于是 $\begin{pmatrix} v_1 \\ v_2 \end{pmatrix}$ 是非迷向的, 而且

$$\begin{pmatrix} v_1 \\ v_2 \end{pmatrix} G \begin{pmatrix} v_1 \\ v_2 \end{pmatrix}' \equiv \begin{pmatrix} a & \\ & a^{-1} \end{pmatrix} \begin{pmatrix} v_2 \\ v_1 \end{pmatrix} G \begin{pmatrix} v_2 \\ v_1 \end{pmatrix}' \begin{pmatrix} a & \\ & a^{-1} \end{pmatrix}.$$

依定理 1, 有 $T \in O_n(F,G)$, 使

$$\begin{pmatrix} v_1 \\ v_2 \end{pmatrix} = \begin{pmatrix} a & \\ & a^{-1} \end{pmatrix} \begin{pmatrix} v_2 \\ v_1 \end{pmatrix} T.$$

于是

$$v_1 = av_2T.$$

其次, 研究 $\nu \neq 0$ 的情形. 这时有 n 维向量 u_1 存在, 使 $v_1Su_1' = 1$. 我们可以假定 $u_1Gu_1' = 0$. 实际上, 如$u_1Gu_1' \neq 0$, 则有 $\beta = \lambda v_1 + \mu v_2 + \xi$, $\xi \in \begin{pmatrix} v_1 \\ u_1 \end{pmatrix}^*$, 使 $\beta G\beta' = 0$. 令 $v_1Su_1' = \mu$. 如 $\mu \neq 0$, 我们可取 $\mu^{-1}\beta$ 作为新的 u_1, 就有 $v_1Su_1' = 1$, 使 $u_1Gu_1' = 0$. 如 $\mu = 0$, 而且 $\lambda = 0$, 有 $\gamma \in \begin{pmatrix} v_1 \\ u_1 \end{pmatrix}^*$, 使 $\gamma G\gamma' = u_1Gu_1'$, 于是可取 $u_1 + \gamma$ 作为新的 u_1. 如 $\mu_1 = 0$ 而且 $\lambda \neq 0$, 则

$$(\lambda v_1 + \lambda(u_1Gu_1')^{-1}u_1 + \xi)G(\lambda v_1 + \lambda(u_1Gu_1')^{-1}u_1 + \xi)' = 0.$$

这又化到 $\mu \neq 0$ 的情形.

同样, 我们可求得一向量 u_2, 使 $v_2Su_2' = 1$, 而 $u_2Gu_2' = 0$. 于是

$$\begin{pmatrix} v_1 \\ u_2 \end{pmatrix} G \begin{pmatrix} v_1 \\ u_2 \end{pmatrix}' = \begin{pmatrix} a & \\ & a^{-1} \end{pmatrix}\begin{pmatrix} v_2 \\ u_2 \end{pmatrix} G \begin{pmatrix} v_2 \\ u_2 \end{pmatrix}' \begin{pmatrix} a & \\ & a^{-1} \end{pmatrix} = \begin{pmatrix} v_1Gv' & 1 \\ & 0 \end{pmatrix}.$$

依定理 1, 有 $T \in O_n(F,G)$, 使

$$\begin{pmatrix} v_1 \\ u_1 \end{pmatrix} = \begin{pmatrix} a & \\ & a^{-1} \end{pmatrix}\begin{pmatrix} v_2 \\ u_2 \end{pmatrix} T.$$

于是

$$v_1 = av_2T.$$

系理 2 设 v_1 和 v_2 是两个非奇异向量, 如 $v_1Gv_1' = v_2Gv_2'$, 则有 $T \in O_n(F,G)$, 使

$$v_1 = v_2T.$$

§4 $O_n(F,G)$ 中元素的形式

先研究 $\nu = \dfrac{n}{2}$ 的情形. 设

$$G = \begin{pmatrix} 0 & I^{(\nu)} \\ 0 & 0 \end{pmatrix}.$$

于是

$$T = \begin{pmatrix} A & B \\ C & D \end{pmatrix}$$

属于 $O_n(F, G)$, 当且仅当

(1) $$AB' \equiv 0,\ \ CD' \equiv 0\ \ 及\ \ AD' + BC' = I.$$

又从 $TGT' \equiv G$ 推出 $T^{-1}GT'^{-1} \equiv G$. 但是

$$T^{-1} = \begin{pmatrix} D' & B' \\ C' & A' \end{pmatrix},$$

故有

(2) $$D'B \equiv 0,\ \ C'A \equiv 0\ \ 及\ \ D'A + B'C' = I.$$

定理 1　当 $\nu = \frac{n}{2}$ 时, 以下这些元素都是 $O_n(F, G)$ 中的元素:

I. $\begin{pmatrix} A & 0 \\ 0 & A'^{-1} \end{pmatrix}$　(A是$\nu \times \nu$可逆阵);

II. $\begin{pmatrix} I & K \\ 0 & I \end{pmatrix}$及$\begin{pmatrix} I & 0 \\ K & 0 \end{pmatrix}$　($K \equiv 0$);

III. $\begin{pmatrix} J & I-J \\ I-J & J \end{pmatrix}$　($J^2 = J$是对角矩阵),

而且, $O_n(F, G)$ 中每一个元素都可以表成下面的形状:

$$\begin{pmatrix} I & 0 \\ X & I \end{pmatrix}\begin{pmatrix} A & 0 \\ 0 & A'^{-1} \end{pmatrix}\begin{pmatrix} I & Y \\ 0 & I \end{pmatrix}\begin{pmatrix} J & I-J \\ I-J & J \end{pmatrix},$$

其中 $X \equiv 0, Y \equiv 0, A$ 可逆, $J^2 = J$ 是对角矩阵.

可仿第七章 §7 证之, 亦可与第九章定理 1.2 比较.

再研究 $0 < 2\nu < n$ 的情形. 设

$$G = \begin{pmatrix} 0 & I^{(\nu)} & \\ 0 & 0 & \\ & & \Delta \end{pmatrix},$$

而

$$\Delta = \begin{pmatrix} \alpha_1 & & & 1 & & \\ & \ddots & & & \ddots & \\ & & \alpha_{\frac{n-2\nu}{2}} & & & 1 \\ & & & \beta_1 & & \\ & & & & \ddots & \\ & & & & & \beta_{\frac{n-2\nu}{2}} \end{pmatrix}$$

是定号的, 即 $x\Delta x' = 0$ 推出 $x = 0$. 这时我们有

定理 2 当 $0 < 2\nu < n$ 时, 以下这些元素都是 $O_n(F, G)$ 中的元素:

I. $\begin{pmatrix} A & B & \\ C & D & \\ & & I \end{pmatrix}$, 而 $\begin{pmatrix} A & B \\ C & D \end{pmatrix} \in O_{2\nu}(F, S_1), S_1 = \begin{pmatrix} 0 & I^{(\nu)} \\ 0 & 0 \end{pmatrix}$;

II. $\begin{pmatrix} I & & \\ & I & \\ & & U \end{pmatrix}$ $(U \in O_{n-2\nu}(F, \Delta))$;

III. $\begin{pmatrix} J & I-J & \\ I-J & J & \\ & & I \end{pmatrix}$ $(J^2 = J$是对角矩阵$)$;

IV. $\begin{pmatrix} I & P\Delta P' & P \\ & I & \\ & (\Delta+\Delta')P' & I \end{pmatrix}$和$\begin{pmatrix} I & & \\ P\Delta P' & I & P \\ (\Delta+\Delta')P' & & I \end{pmatrix}$, 而$P = P^{(\nu, n-2\nu)}$是任意的.

更进一步, $O_n(F, G)$ 中任一元素皆可表示成下面形状:

$$\begin{pmatrix} I & & \\ X\Delta X' & I & X \\ (\Delta+\Delta')X' & & I \end{pmatrix}\begin{pmatrix} A & B & \\ C & D & \\ & & U \end{pmatrix}\begin{pmatrix} I & Y\Delta Y' & P \\ & I & \\ & (\Delta+\Delta')Y' & I \end{pmatrix}\begin{pmatrix} J & I-J & \\ I-J & J & \\ & & I \end{pmatrix}.$$

这个定理可仿第七章 §8 证之, 亦可与第九章定理 1.3 相比较.

§5 正交平延

仍以 S 表示交错矩阵 $G + G'$. 我们在 §3 中已经指出, $O_n(F, G)$ 是 $Sp_n(F, S)$ 的子群. 现在我们来研究, 何时一个辛平延是正交平延.

依第七章定理 9.1, 任一辛平延皆可表作

$$I+\lambda Sv'v,$$

而 $\lambda\in F^*$ 及 $vSv'=0$. 更进一步, 我们有

定理 1 辛平延 $I+\lambda Sv'v$ 是正交矩阵 (因而是正交平延) 当且仅当 v 是非奇异的而且 $\lambda=(vGv')^{-1}$.

【证】 如 v 非奇异, 而且 $\lambda=(vGv')^{-1}$, 则

$$\begin{aligned}&(I+\lambda Sv'v)G(I+\lambda Sv'v)'\\=&G+\lambda Sv'vG+\lambda Gv'vS+\lambda^2Sv'vGv'vS\\\equiv&G+\lambda Sv'vS+\lambda Sv'vS=G,\end{aligned}$$

即 $I+\lambda Sv'v$ 正交.

反之, 如 $I+\lambda Sv'v$ 正交, 则

$$(I+\lambda Sv'v)G(I+\lambda Sv'v)'\equiv G.$$

于是

$$\lambda Sv'vG+\lambda Gv'vS+\lambda^2Sv'vGv'vS\equiv 0,$$

$$\lambda Sv'vS+\lambda^2Sv'(vGv')vS\equiv 0,$$

$$(\lambda+\lambda^2vGv')Sv'vS\equiv 0.$$

如 $vGv'=0$, 即 $Sv'vS=0$, 这是不可能的. 因此 $vGv'\neq 0$. 于是

$$\lambda=(vGv')^{-1}.$$

定理 2 设 $\nu\geqslant 1$, 则任一正交平延皆正交相似于以下形状的一个正交平延:

$$\begin{pmatrix}0&0&\lambda^{-1}&0&0\\0&I^{(\nu-1)}&0&0&0\\\lambda&0&0&0&0\\0&0&0&I^{(\nu-1)}&0\\0&0&0&0&I^{(n-2\nu)}\end{pmatrix}.\tag{1}$$

【证】 设 $I+\lambda Sv'v$ 是正交平延, 而 $\lambda=(vGv')^{-1}$, 则 $vGv'=\lambda^{-1}$. 因

$$(1\ 0\ \lambda^{-1}\ 0\ 0)\begin{pmatrix}0&I&\\0&0&\\&&\Delta\end{pmatrix}(1\ 0\ \lambda^{-1}\ 0\ 0)'=\lambda^{-1},$$

故依定理 3.3 的系理, 有 $T \in O_n(F,G)$, 使

$$v = (1\ 0\ \lambda^{-1}\ 0\ 0)T.$$

于是

$$\begin{aligned} T(I+\lambda Sv'v)T^{-1} &= I+\lambda S(vT^{-1})'(vT^{-1}) \\ &= I+\lambda S(1\ 0\ \lambda^{-1}\ 0\ 0)'(1\ 0\ \lambda^{-1}\ 0\ 0), \end{aligned}$$

即为形状 (1).

定理 3 $O_n(F,G)$ 由正交平延所生成, 除开 $n=4, \nu=2$ 而 $F=F_2$ 这一情形.

证 以 $\mathfrak{T}$ 表示正交平延所生成之群. 先研究 $\nu = \dfrac{n}{2}$ 的情形. 对于任一 $\lambda \in F^*$, 有正交平延

$$\begin{pmatrix} 0 & 0 & \lambda^{-1} & 0 \\ 0 & I & 0 & 0 \\ \lambda & 0 & 0 & 0 \\ 0 & 0 & 0 & I \end{pmatrix}.$$

特别, $\mathfrak{T}$ 包有

$$\begin{pmatrix} 0 & 0 & 1 & 0 \\ 0 & I & 0 & 0 \\ 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & I \end{pmatrix}.$$

因

$$\begin{pmatrix} 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 \\ 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix}\begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 \end{pmatrix} = \begin{pmatrix} 0 & I^{(2)} \\ I^{(2)} & 0 \end{pmatrix},$$

故 $\mathfrak{T}$ 包有

$$\begin{pmatrix} J & I-J \\ I-J & J \end{pmatrix}, \tag{2}$$

对一切对角矩阵 $J=J^2$. 其次, $\mathfrak{T}$ 包有

$$\begin{pmatrix} 0 & 0 & \lambda^{-1} & 0 \\ 0 & I & 0 & 0 \\ \lambda & 0 & 0 & 0 \\ 0 & 0 & 0 & I \end{pmatrix}\begin{pmatrix} 0 & 0 & 1 & 0 \\ 0 & I & 0 & 0 \\ 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & I \end{pmatrix} = \begin{pmatrix} \lambda^{-1} & 0 & 0 & 0 \\ 0 & I & 0 & 0 \\ 0 & 0 & \lambda & 0 \\ 0 & 0 & 0 & I \end{pmatrix}$$

除开 $n=4$ 及 $F=F_2$ 之外, 由第六章定理 3.3 推出 $\mathfrak{T}$ 包有

$$\begin{pmatrix} A & 0 \\ 0 & A'^{-1} \end{pmatrix}, \tag{3}$$

而 $A\in GL_v(F)$. 最后, $\mathfrak{T}$ 包有

$$\begin{pmatrix} I & K \\ 0 & I \end{pmatrix}\begin{pmatrix} A & 0 \\ 0 & A'^{-1} \end{pmatrix}\begin{pmatrix} I & K \\ 0 & I \end{pmatrix}^{-1}\begin{pmatrix} A & 0 \\ 0 & A'^{-1} \end{pmatrix}^{-1}=\begin{pmatrix} I & K-AKA' \\ 0 & I \end{pmatrix}.$$

如 $F\neq F_2$, 设 $a\neq 0,1$, 取

$$A=\begin{pmatrix} a & 0 & \\ 0 & 1 & \\ & & I \end{pmatrix},\quad K=\begin{pmatrix} 0 & 1 & \\ 1 & 0 & \\ & & 0 \end{pmatrix}.$$

我们有

$$K-AKA'=\begin{pmatrix} 0 & a+1 & \\ a+1 & 0 & \\ & & 0 \end{pmatrix}.$$

如 $F=F_2$ 而 $n\geqslant 6$, 取

$$K=\begin{pmatrix} & & 1 & \\ & 0 & & \\ 1 & & & \\ & & & 0 \end{pmatrix},\quad A=\begin{pmatrix} 0 & 1 & \\ 1 & 0 & \\ & & I \end{pmatrix},$$

则

$$K-AKA'=\begin{pmatrix} 0 & 0 & 1 & \\ 0 & 0 & 1 & \\ 1 & 1 & 0 & \\ & & & 0 \end{pmatrix}.$$

在这两个情形, $\mathfrak{T}$ 都包有一个形如

$$\begin{pmatrix} I & K \\ 0 & I \end{pmatrix}$$

的元素, 其中 $K\equiv 0$, 而且 K 的秩为 2. 因

$$\begin{pmatrix} I & K_1 \\ 0 & I \end{pmatrix}\begin{pmatrix} I & K_2 \\ 0 & I \end{pmatrix}=\begin{pmatrix} I & K_1+K_2 \\ 0 & I \end{pmatrix},$$

$$\begin{pmatrix} P & 0 \\ 0 & P'^{-1} \end{pmatrix}\begin{pmatrix} I & K \\ 0 & I \end{pmatrix}\begin{pmatrix} P & 0 \\ 0 & P'^{-1} \end{pmatrix}^{-1} = \begin{pmatrix} I & PKP' \\ 0 & I \end{pmatrix},$$

故 $\mathfrak{T}$ 包有一切

(4) $$\begin{pmatrix} I & K \\ 0 & I \end{pmatrix} \qquad (K \equiv 0).$$

依定理 4.1, $O_n(F, G)$ 由一切 (2), (3), (4) 所生成. 故 $\mathfrak{L} = O_n(F, G)$.

再研究 $\nu < \dfrac{n}{2}$ 的情形. 我们先证明, $\mathfrak{T}$ 包有一切

(5) $$\begin{pmatrix} A & B & \\ C & D & \\ & & I \end{pmatrix}, \quad \begin{pmatrix} A & B \\ C & D \end{pmatrix} \in O_{2\nu}\left(F, \begin{pmatrix} 0 & I^{(\nu)} \\ 0 & 0 \end{pmatrix}\right).$$

如 $F \neq F_2$ 或 $F = F_2$ 而 $\nu \geqslant 3$, 这是情形 $\nu = \dfrac{n}{2}$ 的结论. 如 $F = F_2$ 而 $\nu = 2$, 可如下进行: 首先, 我们指出, 容易证明 $n = 6$ 而且可设

$$\Delta = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}.$$

注意 (0 0 0 0 1 0) 及 (0 0 0 1 1 0) 都是奇异向量, 以它们为向量的正交平延设为 T_1 和 T_2, 则 $\mathfrak{T}$ 包有

$$T_1T_2 = \begin{pmatrix} I & P\Delta P' & P \\ & I & \\ & (\Delta + \Delta')P & I \end{pmatrix},$$

而 $P = \begin{pmatrix} 0 & 0 \\ 1 & 0 \end{pmatrix}$. 因

$$\begin{pmatrix} A & & \\ & A'^{-1} & \\ & & I \end{pmatrix}\begin{pmatrix} I & P\Delta P' & P \\ & I & \\ & (\Delta + \Delta')P & I \end{pmatrix}\begin{pmatrix} A & & \\ & A'^{-1} & \\ & & I \end{pmatrix}^{-1}$$

$$= \begin{pmatrix} I & AP\Delta P'A' & AP \\ & I & \\ & (\Delta + \Delta')P'A' & I \end{pmatrix},$$

故 $\mathfrak{T}$ 也包有

$$\begin{pmatrix} I & P_i\Delta P_i' & P_i \\ & I & \\ & (\Delta + \Delta')P_i' & I \end{pmatrix} \quad (i = 1, 2),$$

而 $P_1=\begin{pmatrix}1&0\\0&0\end{pmatrix}$ 及 $P_2=\begin{pmatrix}1&0\\1&0\end{pmatrix}$. 我们有

$$\begin{pmatrix}I&P\Delta P'&P\\&I&\\&(\Delta+\Delta')P&I\end{pmatrix}\begin{pmatrix}I&P_1\Delta P_1'&P_1\\&I&\\&(\Delta+\Delta')P_2'&I\end{pmatrix}$$

$$=\begin{pmatrix}I&P_2\Delta P_2'&P_2\\&I&\\&(\Delta+\Delta')P_2'&I\end{pmatrix}\begin{pmatrix}I&K&\\&I&\\&&I\end{pmatrix},$$

而 $K=\begin{pmatrix}0&1\\1&0\end{pmatrix}$. 因之 $\mathfrak{T}$ 包有

$$\begin{pmatrix}I&K&\\0&I&\\&&I\end{pmatrix}$$

以及

$$\left[\begin{pmatrix}I&I&\\I&0&\\&&I\end{pmatrix}\begin{pmatrix}I&K&\\0&I&\\&&I\end{pmatrix}\right]^3=\begin{pmatrix}K&0&\\0&K&\\&&I\end{pmatrix}.$$

所以 $\mathfrak{T}$ 包有

$$\begin{pmatrix}A&0&\\0&A'^{-1}&\\&&I\end{pmatrix}\quad(A\in GL_2(F)).$$

像情形 $\nu=\dfrac{n}{2}$ 一样进行下去, 即可推出我们的断言.

其次, 因

$$\begin{pmatrix}I&P\Delta P'&P\\&I&\\&(\Delta+\Delta')P'&I\end{pmatrix}\begin{pmatrix}I&Q\Delta Q'&Q\\&I&\\&(\Delta+\Delta')Q'&I\end{pmatrix}$$

$$=\begin{pmatrix}I&(P+Q)\Delta(P+Q)'&P+Q\\&I&\\&(\Delta+\Delta')(P+Q)'&I\end{pmatrix}\begin{pmatrix}I&Q\Delta P'+P\Delta'Q'&\\&I&\\&&I\end{pmatrix},$$

而 $Q\Delta P'+P\Delta'Q'$ 是交错矩阵. 因此, 需证 $\mathfrak{T}$ 包有一切

$$(6)\qquad \begin{pmatrix} I & P\Delta P' & P \\ & I & \\ & (\Delta+\Delta')P' & I \end{pmatrix}$$

只要证 $\mathfrak{T}$ 包有形如 (6) 的元素中

$$P=\begin{pmatrix} & 0 & \\ 0\cdots 0 & p & 0\cdots 0 \\ & 0 & \end{pmatrix}$$

即可. 如 $F=F_2$, 这可从上一段的讨论中推出. 如 $F\neq F_2$, 则有 $\lambda\in F^*$ 而 $\lambda\neq 1$. $\mathfrak{T}$ 包有 (为书写简单起见, 设$n=4,\nu=1,\Delta=\begin{pmatrix}\alpha & 1\\ 0 & \beta\end{pmatrix}$)

$$\begin{pmatrix}\lambda & & \\ & \lambda^{-1} & \\ & & I\end{pmatrix}\begin{pmatrix}1 & \alpha p^2 & p & 0\\ 0 & 1 & & \\ & 0 & & \\ & & & I\\ & p & & \end{pmatrix}\begin{pmatrix}\lambda & & \\ & \lambda^{-1} & \\ & & I\end{pmatrix}^{-1}\begin{pmatrix}1 & \alpha p^2 & p & 0\\ 0 & 1 & & \\ & 0 & & \\ & & & I\\ & p & & \end{pmatrix}^{-1}$$

$$=\begin{pmatrix}1 & (\lambda^2+1)\alpha p^2 & (\lambda+1)p & 0\\ 0 & 1 & & \\ & 0 & & \\ & & & I\\ & (\lambda+1)p & & \end{pmatrix}$$

因 $\lambda\neq 1$, 当 p 跑过 F 时, $(\lambda+1)p$ 亦然. 因而断言成立.

依定理 4.2, $O_n(F,G)$ 由一切元素 (5), (6) 及

$$(7)\qquad \begin{pmatrix} I & & \\ & I & \\ & & U \end{pmatrix},$$

而 $U\Delta U'=\Delta$, 所生成, 因此还要证明 (7) 也属于 $\mathfrak{T}$. 我们将这个特殊情形陈述成一条引理.

引理 1 设 G 是无亏数的正则定号矩阵, 则 $O_n(F,G)$ 中任一元素皆是正交平延之积.

【证】 因 G 定号, 所有向量都是非奇异的, 于是对于任一非零向量 v, 都有一个正交平延

$$T=I+(vGv')^{-1}Sv'v.$$

设 U 是一个正交矩阵而 $U \neq I$, 则至少有一个非 0 向量 x 存在, 使 $xU \neq x$. 于是

$$0 \neq (x+xU)G(x+xU)' = xGx' + xG(xU)' + xUGx' + xUG(xU)' = xS(xU)'.$$

令

$$T = I + \lambda S(x+xU)'(x+xU)$$

是一正交平延, 而 $\lambda = [(x+xU)G(x+xU)']^{-1}$, 则 $xT = xU$, 即 $U_1 = UT$ 将 x 保持不变.

至少存在一个非 0 向量 y, 使 $xSy' \neq 0$. 如 $yU_1 = y$, 定义 $U_2 = U_1$. 如 $yU_1 \neq y$, 则

$$xS(y+yU_1)' = 0.$$

于是正交平延

$$T_1 = I + [(y+yU_1)G(y+yU_1)']^{-1}S(y+yU_1)'(y+yU_1)$$

将 x 不动而将 y 变到 yU_1. 定义 $U_2 = U_1T_1$. 在这两个情形都有

$$xU_2 = x, \quad yU_2 = y.$$

平面 $\begin{pmatrix} x \\ y \end{pmatrix}$ 是非迷向的, 于是 $\begin{pmatrix} x \\ y \end{pmatrix}^*$ 也是非迷向的, 而且 U_2 将 $\begin{pmatrix} x \\ y \end{pmatrix}^*$ 变到自身. 对于一组由 x, y 及 $\begin{pmatrix} x \\ y \end{pmatrix}^*$ 中 $n-2$ 个向量所组成的基, U_2 有形状

$$\begin{pmatrix} I^{(2)} & 0 \\ 0 & U_3 \end{pmatrix}.$$

将上述讨论方法应用于 U_3, 如此进行下去, 引理即得证.

作为以上讨论的应用, 我们来确定 $O_n(F,G)$ 的中心.

定理 4　$O_n(F,G)$ 的中心仅由单位矩阵组成, 除开 $n=2, \nu=1, F=F_2$ 这一情形, 而在后一情形 $O_2\left(F_2, \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix}\right)$ 是 2 阶 Abel 群.

【证】　设

$$Z = \begin{pmatrix} A & B & P \\ C & D & Q \\ R & T & U \end{pmatrix}$$

是 $O_n(F,G)$ 的一个中心元素, 因它与所有形如

$$\begin{pmatrix} I & & \\ & I & \\ & & H \end{pmatrix} \quad (H\Delta H' \equiv \Delta)$$

的正交平延交换, 它必为形状

$$Z = \begin{pmatrix} A & B & \\ C & D & \\ & & I \end{pmatrix}.$$

如 $\nu = 0$, 本定理自然成立. 以下设 $\nu > 0$; 我们区别以下两种情形:

(i) $\nu \geqslant 2$. 因 Z 与一切

$$\begin{pmatrix} I & & \\ K & I & \\ & & I \end{pmatrix} \text{及} \begin{pmatrix} I & K & \\ & I & \\ & & I \end{pmatrix} \quad (K \equiv 0)$$

交换, 故 Z 必为形状

$$Z = \begin{pmatrix} A & 0 & \\ 0 & A'^{-1} & \\ & & I \end{pmatrix}.$$

因 Z 与一切

$$\begin{pmatrix} D & 0 & \\ 0 & D'^{-1} & \\ & & I \end{pmatrix} \quad (D \in GL_v(F))$$

交换, 故 Z 必为形状

$$Z = \begin{pmatrix} \lambda I & 0 & \\ 0 & \lambda^{-1} I & \\ & & I \end{pmatrix}.$$

再从

$$\begin{pmatrix} \lambda I & & \\ & \lambda^{-1} I & \\ & & I \end{pmatrix} \begin{pmatrix} 0 & I & \\ I & 0 & \\ & & I \end{pmatrix} = \begin{pmatrix} 0 & I & \\ I & 0 & \\ & & I \end{pmatrix} \begin{pmatrix} \lambda I & & \\ & \lambda^{-1} I & \\ & & I \end{pmatrix},$$

推出 $\lambda = \lambda^{-1}$, 即 $\lambda = 1$.

(ii) $\nu = 1$. 因 $ZGZ' \equiv G, Z$ 必为形状

$$Z = \begin{pmatrix} a & 0 & \\ 0 & a^{-1} & \\ & & I \end{pmatrix} \text{ 或 } \begin{pmatrix} 0 & b & \\ b^{-1} & 0 & \\ & & I \end{pmatrix}.$$

因 Z 与

$$\begin{pmatrix} 0 & 1 & \\ 1 & 0 & \\ & & I \end{pmatrix}$$

交换, 故 Z 必为形状

$$\begin{pmatrix} 1 & 0 & \\ 0 & 1 & \\ & & I \end{pmatrix} \text{ 或 } \begin{pmatrix} 0 & 1 & \\ 1 & 0 & \\ & & I \end{pmatrix}.$$

如 $F \neq F_2$, 有 $a \neq 0, 1$ 存在, 于是有

$$\begin{pmatrix} 0 & 1 & \\ 1 & 0 & \\ & & I \end{pmatrix} \begin{pmatrix} a & 0 & \\ 0 & a^{-1} & \\ & & I \end{pmatrix} \neq \begin{pmatrix} a & 0 & \\ 0 & a^{-1} & \\ & & I \end{pmatrix} \begin{pmatrix} 0 & 1 & \\ 1 & 0 & \\ & & I \end{pmatrix}.$$

如 $F = F_2$, 但 $n \geqslant 4$, 则有 (为书写简单起见, 设 $n = 4$)

$$\begin{pmatrix} 0 & 1 & \\ 1 & 0 & \\ & & I \end{pmatrix} \begin{pmatrix} 1 & 1 & 1 & 0 \\ & 1 & & \\ & 0 & 1 & \\ & 1 & & 1 \end{pmatrix} \neq \begin{pmatrix} 1 & 1 & 1 & 0 \\ & 1 & & \\ & 0 & 1 & \\ & 1 & & 1 \end{pmatrix} \begin{pmatrix} 0 & 1 & \\ 1 & 0 & \\ & & I \end{pmatrix}.$$

因此 $Z = I$, 除非 $F = F_2$, $n = 2$ 而 $\nu = 1$.

§6 由 2 平延所演成的群 (与第九章 §2 相比较)

在本节中我们假定 $\nu \geqslant 2$.

定义 1 正交群 $O_n(F, G)$ 中的一个元素 $T = I + N$ 称为 (正交)2 平延, 如果 N 的秩是 2 而且 $NGN' \equiv 0$.

从 $(I + N)G(I + N)' \equiv G$ 推出 $NG + GN' \equiv 0$. 写

$$N = (N_{ij})_{1 \leqslant i,j \leqslant 4},$$

于是 $NG+GN' \equiv 0$, 给出 $N_{12} \equiv 0, N_{21} \equiv 0, N_{34} \equiv 0, N_{43} \equiv 0$. 再从 $NG+GN' \equiv 0$ 推出 $NS+SN'=0$, 即 NS 对称. 可是

$$NS = \begin{pmatrix} N_{12} & N_{11} & N_{14} & N_{13} \\ N_{22} & N_{21} & N_{24} & N_{23} \\ N_{32} & N_{31} & N_{34} & N_{33} \\ N_{42} & N_{41} & N_{44} & N_{43} \end{pmatrix},$$

故 NS 交错. 因 NS 的秩为 2, 故可写

$$NS = \begin{pmatrix} x_1 \\ x_2 \end{pmatrix}' \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} x_1 \\ x_2 \end{pmatrix}.$$

于是

$$N = \begin{pmatrix} x_1 \\ x_2 \end{pmatrix}' \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} x_1 \\ x_2 \end{pmatrix} S.$$

令

$$\begin{pmatrix} x_1 \\ x_2 \end{pmatrix} S = \begin{pmatrix} v_1 \\ v_2 \end{pmatrix},$$

则有

$$N = S \begin{pmatrix} v_1 \\ v_2 \end{pmatrix}' \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} v_1 \\ v_2 \end{pmatrix}.$$

因之任一 2 平延皆可表作

$$T = I + S \begin{pmatrix} v_1 \\ v_2 \end{pmatrix}' \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} v_1 \\ v_2 \end{pmatrix}.$$

因 $NGN' \equiv 0$, $\begin{pmatrix} v_1 \\ v_2 \end{pmatrix}$ 是全奇异的.

定理 1 在 $O_n(F,G)$ 之下, 任一 2 平延皆相似于

$$\begin{pmatrix} I & K & \\ 0 & I & \\ & & I \end{pmatrix}, \quad K = \begin{pmatrix} 0 & 1 & \\ 1 & 0 & \\ & & 0 \end{pmatrix};$$

也相似于

$$\begin{pmatrix} A & & \\ & A'^{-1} & \\ & & I \end{pmatrix}, \quad A = \begin{pmatrix} 1 & 1 & \\ & 1 & \\ & & I \end{pmatrix}.$$

可仿第九章定理 2.1 的证明证之.

今后, 我们用 $\mathfrak{F}$ 表示 $O_n(F,G)$ 中由 2 平延所演成的子群. 显然, $\mathfrak{F}$ 是 $O_n(F,G)$ 的正规子群.

定理 2 以下这些元素都是 $\mathfrak{F}$ 的元素:

I. $\begin{pmatrix} A & 0 & \\ 0 & A'^{-1} & \\ & & I \end{pmatrix}$ $(\det A \in F^{*2})$;

II. $\begin{pmatrix} I & K & \\ & I & \\ & & I \end{pmatrix}$ 及 $\begin{pmatrix} I & & \\ K & I & \\ & & I \end{pmatrix}$ $(K \equiv 0)$;

III. $\begin{pmatrix} I+J & J & \\ J & I+J & \\ & & I \end{pmatrix}$ ($J^2 = J$为偶秩的对角矩阵);

IV. $\begin{pmatrix} I & P\Delta P' & P \\ & I & \\ & (\Delta+\Delta')P' & I \end{pmatrix}$ 和 $\begin{pmatrix} I & & \\ P\Delta P' & I & P \\ (\Delta+\Delta')P' & & I \end{pmatrix}$,

其中 P 是任意 $\nu \times (m-2\nu)$ 矩阵.

可仿第九章定理 2.2 的证明证之.

定理 3 给了任意一个 $U \in O_{n-2\nu}(F,S)$, F^* 里就有一个元素 a 存在, 使

$$\begin{pmatrix} a & & & & \\ & I & & & \\ & & a^{-1} & & \\ & & & I & \\ & & & & U \end{pmatrix} \text{ 或 } \begin{pmatrix} 0 & & a & & \\ & I & & & \\ a^{-1} & & 0 & & \\ & & & I & \\ & & & & U \end{pmatrix}$$

属于 $\mathfrak{F}$.

利用恒等式

$$\begin{pmatrix} I & p\Delta p' & p \\ & 1 & \\ & (\Delta+\Delta')p' & I \end{pmatrix}\begin{pmatrix} 1 & & \\ q\Delta q' & 1 & q \\ (\Delta+\Delta')q' & & I \end{pmatrix}\begin{pmatrix} 1 & p\Delta p' & p \\ & 1 & \\ & (\Delta+\Delta')p' & I \end{pmatrix}$$

$$= \begin{pmatrix} & p\Delta p' & \\ (p\Delta p')^{-1} & & \\ & & I + S(p\Delta p')^{-1}p'p \end{pmatrix}$$

其中 $q = (p\Delta p')^{-1}p$, 仿照第九章定理 2.3 的证明证之.

定理 4 当 $\nu \geqslant 2$ 时, $\Omega_n(F,G) = \mathfrak{Z}$, 除开 $F = F_2, n = 4, \nu = 2$ 这一情形.

可仿第九章定理 2.4 的证明证之.

§7 由双曲旋转的平方所演成的群 (与第九章 §3 相比较)

在本节中我们假定 $\nu \geqslant 1$.

定义 1 设 P 是个非迷向平面. 如果 P 包含两条奇异直线, 则 P 称为双曲平面. $O_n(F,G)$ 中的一个元素, 如将 P^* 中所有向量皆一个一个地保持不动, 就称为以 P^* 为轴, 以 P 为双曲平面的双曲旋转.

定理 1 设 $\nu \geqslant 1$. 在 $O_n(F,G)$ 之下, 双曲旋转一定相似于下面形状的一个元素:

$$\begin{pmatrix} a & & & & \\ & I & & & \\ & & a^{-1} & & \\ & & & I & \\ & & & & I \end{pmatrix} \text{ 或 } \begin{pmatrix} & & a & & \\ & I & & & \\ a^{-1} & & & & \\ & & & I & \\ & & & & I \end{pmatrix}.$$

可仿第九章定理 3.1 的证明证之.

定理 2 设 $\nu \geqslant 1$. 则每个正交矩阵都是双曲旋转之积, 除开 $F = F_2, n = 4, \nu = 2$ 这一情形.

证 因当 $\nu \geqslant 1$ 时, 正交平延都是双曲旋转, 故本定理是定理 5.3 的推论.

以下我们除开 $F = F_2$ 这一情形. 我们用 $\mathfrak{H}$ 表 $O_n(F,G)$ 中由双曲旋转的平方所演成之群. 显然, $\mathfrak{H}$ 是 $O_n(F,G)$ 的正规子群.

定理 3 若 $v \geqslant 1$ 而 $F \neq F_2$, 以下这些元素都是 $\mathfrak{H}$ 的元素:

I. $$\begin{pmatrix} A & 0 & \\ 0 & A'^{-1} & \\ & & I \end{pmatrix} \quad (\det A \in F^{*2});$$

II. $$\begin{pmatrix} I & K & \\ 0 & I & \\ & & I \end{pmatrix} \quad (K \equiv 0, \text{或} \nu \geqslant 2);$$

III. $$\begin{pmatrix} I+J & J & \\ J & I+J & \\ & & I \end{pmatrix} \quad (J^2 - J\text{是偶秩的对角阵, 若}\nu \geqslant 2)$$

IV. $\begin{pmatrix} I & P\Delta P' & P \\ & I & \\ & (\Delta+\Delta')P' & I \end{pmatrix}$ (P为任意$\nu \times (n-2\nu)$矩阵).

可仿第九章定理 2.2 及 3.2 的证明证之.

定理 4　设 $\nu \geqslant 1$ 而 $F \neq F_2$, 则 $\Omega_n(F, G) = \mathfrak{H}$.

可仿第九章定理 2.4 的证明证之.

§8　$O_n(F, G)$ 的构造 $(\nu \geqslant 1)$

定理 1　设 $n \geqslant 4$ 及 $\nu \geqslant 1$. 则群 $\Omega_n(F, G)$ 是单群, 除开以下的例外:

$$\Omega_4\left(F, \begin{pmatrix} 0 & I \\ 0 & 0 \end{pmatrix}\right).$$

因为 F_2 上的 $n \times n$ 正则矩阵的指数总 > 1, 若 $n \geqslant 6$. 所以只要分别研究以下三种情形:

(i) $n \geqslant 4, \nu = 1, F \neq F_2$.

(ii) $n \geqslant 6, \nu \geqslant 2$.

(iii) $\Omega_4\left(F_2, \begin{pmatrix} 0 & 1 & & \\ 0 & 0 & & \\ & & 1 & 1 \\ & & 0 & 1 \end{pmatrix}\right)$.

情形 (i) 的讨论可仿第九章 §6 证之, 而情形 (ii) 的讨论可仿第九章 §7 证之. 而情形 (iii) 可参看 Dickson, Linear Groups.

最后, 仿照第七章定理 11.1 的证明可证

定理 2　设 $q = 2^n$. 以 F_q 表示 q 个元素的有限域. 于是群 $O_{2m}(F_q, G) = \Omega_{2m}(F_q, G)$ 的阶, 当 G 的指数 $\nu = m$ 时, 为

$$(q^m - 1)(q^{2(m-1)} - 1)q^{2(m-1)} \cdots (q^2 - 1)q^2,$$

当 G 的指数 $\nu = m - 1$ 时, 为

$$(q^m + 1)(q^{2(m-1)} - 1)q^{2(m-1)} \cdots (q^2 - 1)q^2.$$

第十一章 特征数为 2 的域上有亏数的正交群

§1 群 $O_n(F,G)$ 的一些初步性质

在本章中我们仍假定 F 是特征数为 2 的域, 并且总假定 G 是个亏数 $d>0$ 的 $n\times n$ 正则矩阵. 在第十章 §3 中已经定义, 一切适合条件 $TGT'\equiv G$ 的矩阵 T 组成一群, 称为 F 上对 G 而言的正交群, 记作 $O_n(F,G)$.

我们可以写

$$G=\begin{pmatrix} G_1^{(2p)} & \\ & G_2^{(d)} \end{pmatrix} \quad (2p+d=n),$$

其中 G_1 是个无亏数的正则矩阵, 而 G_2 是正则对角矩阵. 相应地, 我们写

$$T=\begin{pmatrix} A & B \\ C & D \end{pmatrix}.$$

其中 $A=A^{(2p)}, B=B^{(2p,d)}, C=C^{(d,2p)}, D=D^{(d)}$. 于是从 $TGT'\equiv G$ 推出

(1) $$AG_1A'+BG_2B'\equiv G_1,$$

(2) $$CG_1C'+DG_2D'\equiv G_2$$

及

(3) $$AG_1C'+BG_2D'+(C_1G_1A'+DG_2B')'=0.$$

从 (1) 推出

$$A(G_1+G_1')A'=G_1+G_1',$$

即 A 是对于可逆交错矩阵 G_1+G_1' 的辛矩阵, 因之 A 可逆. 从 (3) 推出

$$A(G_1+G_1')C'=0.$$

因 A 可逆, G_1 无亏数, 故 $C=0$. 再从 (2) 推出

$$(D+I)G_2(D+I)'\equiv 0,$$

因 G_2 是正则对角矩阵, 故 $D=I$. 因之, 如 $T\in O_n(F,G)$, 则

(4) $$T=\begin{pmatrix} A & B \\ 0 & I \end{pmatrix},$$

而 A 为对于 G_1+G_1' 的辛矩阵, 而且

(5) $$AG_1A' + G_1 \equiv BG_2B'.$$

反之, 如 A 是对于 $G_1 + G_1'$ 的辛矩阵, 而 A, B 适合条件 (5), 则 (4) 是 $O_n(F, G)$ 中的元素. 更进一步, 矩阵 B 由 A 唯一确定. 实际上, 从 $AG_1A' + G_1 \equiv BG_2B'$ 及 $AG_1A' + G \equiv B_1G_2B_1'$ 推出 $(B + B_1)G_2(B + B_1)' \equiv 0$, 因之 $B = B_1'$. 这样我们证明了

定理 1　群 $O_n(F, G)$ 与 $Sp_{2p}(F, G_1 + G_1')$ 的一个子群同构, 这个子群由那些辛矩阵 A 所组成, 这种辛矩阵 A 具有性质

$$AG_1A' + G_1 \equiv BG_2B',$$

对于某个唯一确定的 B.

为了简单起见, 以下我们就用 $O_n(F, G)$ 表 $Sp_{2p}(F, G_1 + G_1')$ 的这个子群.

从 (1) 容易看出, $AG_1A' + G_1$ 和 BG_2B' 都与对角矩阵合同. 因此只需描写 $AG_1A' + G_1$ 的对角元素. 令

$$G_2 = [\delta_1, \delta_2, \cdots, \delta_d].$$

考虑加法子群

$$\mathfrak{M} = F^2\delta_1 + F^2\delta_2 + \cdots + F^2\delta_d,$$

其中 F^2 表示 F 中平方元素所组成的域. 因 G_2 正则, $\mathfrak{M}$ 是 F^2 上的 d 维向量空间. 于是我们有

定理 2　群 $O_n(F, G)$ 由 $Sp_{2p}(F, G_1 + G_1')$ 中那些元素 A 组成, 它具有性质:

$$AG_1A' + G_1$$

的对角线元素属于 $\mathfrak{M}$.

【证】　因 $\delta_1, \delta_2, \cdots, \delta_d$ 在 F^2 上线性无关, B 由 $AG_1A' + G_1$ 的对角线元素唯一确定.

系理 1　如 $p = 0$, 群 $O_n(F, G)$ 仅由单位元素组成. 如 $p > 0$, 群 $O_n(F, G)$ 包有 $O_{2p}(F, G_1)$ 作为子群, 因之, $O_n(F, G)$ 的中心仅由单位元素组成.

系理 2　如 $\mathfrak{M} = F$, 则群 $O_n(F, G)$ 与 $Sp_{2p}(F)$ 相重.

最后, 我们给出一个重要注意. 如 F 为有限域, 或更一般地, F 为完全域. 即 $F^2 = F$, 则 $\mathfrak{M} = F$, 因之这时 $O_n(F, G) = Sp_{2p}(F)$. 因为群 $Sp_{2p}(F)$ 已研究过, 所以以下我们将永远假定 F 不是完全域, 因此 F 不是有限域.

§2　半奇异向量

定义 1　一个 $2p$ 维向量 v 称为:

I. 奇异, 如 $vG_1v'=0$;

II. 半奇异, 如 $vG_1v'\in\mathfrak{M}$;

III. 非奇异, 如 $vG_1v'\neq 0$.

显然, 奇异向量一定半奇异, 但半奇异向量或是奇异, 或是非奇异.

奇异向量只在 G_1 的指数 $\nu\geqslant 1$ 时才存在.

定理 1 如果有半奇异向量存在, 则 G 的指数 >0.

【证】 从 $vG_1v'\in\mathfrak{M}$ 推出有一个 d 维向量 u, 使 $vG_1v'=uG_2u'$. 于是 (v,u) 就是 G 的一个奇异向量. 因此 $\nu\geqslant 1$.

定理 2 正交矩阵将半奇异向量变到半奇异向量.

【证】 设 v 是半奇异向量, 即 $vG_1v'\in\mathfrak{M}$, 设 A 是正交变换, 即 $AG_1A'+G_1\equiv B$, 而 B 是对角形矩阵其对角线元素皆属于 $\mathfrak{M}$. 于是

$$(vA)G_1(vA)'=vAG_1A'v'=v(G_1+B)v'=vG_1v'+vBv'$$

仍属于 $\mathfrak{M}$, 因此本定理成立.

定理 3 设 v_1 和 v_2 是两个任意的半奇异向量, 则有一正交矩阵 A, 使

$$v_1=v_2A.$$

【证】 设 u_1 和 u_2 是 d 维向量, 使

$$u_1G_2u_1'=v_1G_1v_1',\ u_2G_2u_2'=v_2G_1v_2',$$

则

$$(v_1,u_1)G(v_1,u_1)'=0,\quad (v_2,u_2)G(v_2,u_2)'=0.$$

有 $(n-1)\times n$ 矩阵 Y_1 和 Y_2 存在, 使

$$\begin{pmatrix} v_1 & u_1 \\ \multicolumn{2}{c}{Y_1} \end{pmatrix} \text{和} \begin{pmatrix} v_2 & u_2 \\ \multicolumn{2}{c}{Y_2} \end{pmatrix}$$

皆可逆. 于是

$$\begin{pmatrix} v_1 & u_1 \\ \multicolumn{2}{c}{Y_1} \end{pmatrix} G \begin{pmatrix} v_1 & u_1 \\ \multicolumn{2}{c}{Y_1} \end{pmatrix}' = \begin{pmatrix} 0 & (v_1,u_1)(G+G')Y_1' \\ 0 & Y_1GY_1' \end{pmatrix}$$

$$\begin{pmatrix} v_2 & u_2 \\ \multicolumn{2}{c}{Y_2} \end{pmatrix} G \begin{pmatrix} v_2 & u_2 \\ \multicolumn{2}{c}{Y_2} \end{pmatrix}' = \begin{pmatrix} 0 & (v_2,u_2)(G+G')Y_2' \\ 0 & Y_2GY_2' \end{pmatrix}$$

因 G 正则, $(v_1,u_1)(G+G')Y_1'$ 和 $(v_2,u_2)(G+G')Y_2'$ 都是非 0 向量. 因此有

$(n-1)\times(n-1)$ 可逆矩阵 P_1 和 P_2 存在, 使

$$\begin{pmatrix} 1 & \\ & P_i \end{pmatrix}\begin{pmatrix} v_i & u_i \\ & Y_i \end{pmatrix} G \begin{pmatrix} v_i & u_i \\ & Y_i \end{pmatrix}' \begin{pmatrix} 1 & \\ & P_i \end{pmatrix}' = \begin{pmatrix} 0 & 1 & 0\cdots 0 \\ 0 & a_i & b_i \\ 0 & 0 & \\ \vdots & \vdots & D_i \\ 0 & 0 & \end{pmatrix} \quad (i=1,2).$$

于是

$$\begin{pmatrix} 1 & & \\ a_i & 1 & \\ b_i' & & I \end{pmatrix}\begin{pmatrix} 0 & 1 & \\ & a_i & b_i \\ & & D_i \end{pmatrix}\begin{pmatrix} 1 & & \\ a_i & 1 & \\ b_i' & & I \end{pmatrix}' = \begin{pmatrix} 0 & 1 & 0 \\ 0 & 0 & 0 \\ 0 & 0 & D_i \end{pmatrix} \quad (i=1,2).$$

根据 Witt 定理的推广 (第十章定理 1.4), 推出 D_1 和 D_2 合同, 即有 $(n-2)\times(n-2)$ 可逆矩阵 R 存在, 使 $RD_1R' = D_2$. 于是

$$\left[\begin{pmatrix} 1 & & \\ a_2 & 1 & \\ b_2' & & I \end{pmatrix}\begin{pmatrix} 1 & \\ & P_2 \end{pmatrix}\begin{pmatrix} v_2 & u_2 \\ & Y_2 \end{pmatrix}\right]^{-1}\begin{pmatrix} I & \\ & R \end{pmatrix}\begin{pmatrix} 1 & & \\ a_1 & 1 & \\ b_1' & & I \end{pmatrix}$$
$$\cdot\begin{pmatrix} 1 & \\ & P_1 \end{pmatrix}\begin{pmatrix} v_1 & u_1 \\ & Y_1 \end{pmatrix} = \begin{pmatrix} A^{(2p)} & B \\ & I \end{pmatrix}$$

有性质 $AG_1A' + G_1 \equiv BG_2B'$, 而且

$$v_1 = v_2A,$$

而 $A \in O_n(F,G)$. 定理证毕.

系理　如 v_1 是一个半奇异向量, 而 v_2 是任一奇异向量, 则有一正交矩阵 A, 使

$$v_1 = v_2A.$$

定理 4　设 v_1, v_2 是两个非奇异向量. 如 $v_1G_1v_1' = v_2G_1v_2'$, 则有一正交矩阵 A, 使

$$v_1 = v_2A.$$

【证】　这从 $O_n(F,G) \supseteq O_{2p}(F,G_1)$ 及关于 $O_{2p}(F,G_1)$ 的相关结果 (第十章定理 3.3 的系理) 推出.

定理 5 设 v_1, w_1, v_2, w_2 是半奇异向量. 如果 $v_1Sw_1' = v_2Sw_2'$, 而 $S = G_1+G_1'$, 则有一正交矩阵 A, 使

$$\begin{pmatrix} v_1 \\ w_1 \end{pmatrix} = \begin{pmatrix} v_1 \\ w_1 \end{pmatrix} A.$$

【证】 存在着 d 维向量 x_1, y_1, x_2, y_2, 使

$$(v_1, x_1)G(v_1, x_1)' = 0,\ (v_2, x_2)G(v_2, x_2)' = 0,$$
$$(w_1, y_1)G(w_1, y_1)' = 0,\ (w_2, y_2)G(w_2, y_2)' = 0.$$

于是

$$\begin{pmatrix} v_1 & x_1 \\ w_1 & y_1 \end{pmatrix} G \begin{pmatrix} v_1 & x_1 \\ w_1 & y_1 \end{pmatrix}' \equiv \begin{pmatrix} 0 & v_1Sw_1' \\ 0 & 0 \end{pmatrix}$$
$$\equiv \begin{pmatrix} v_2 & x_2 \\ w_2 & y_2 \end{pmatrix} G \begin{pmatrix} v_2 & x_2 \\ w_2 & y_2 \end{pmatrix}'.$$

分别讨论以下两种情形:

(i)$v_1Sw_1' = v_2Sw_2' = 0$. 这时可像定理 3 的证明那样来证明本定理.

(ii)$v_1Sw_1' = v_2Sw_2' \neq 0$. 这时, $\begin{pmatrix} v_1 \\ w_1 \end{pmatrix}$ 和 $\begin{pmatrix} v_2 \\ w_2 \end{pmatrix}$ 是对于 $S = G_1 + G_1'$ 的非迷向平面, 于是

$$\begin{pmatrix} v_i & x_i \\ w_i & y_i \\ \begin{pmatrix} v_i \\ w_i \end{pmatrix}^* & \\ & I \end{pmatrix} G \begin{pmatrix} v_i & x_i \\ w_i & y_i \\ \begin{pmatrix} v_i \\ w_i \end{pmatrix}^* & \\ & I \end{pmatrix}'$$

$$\equiv \begin{pmatrix} \begin{matrix} 0 & v_iSw_i' \\ 0 & 0 \end{matrix} & 0 & \\ 0 & \begin{pmatrix} v_i \\ w_i \end{pmatrix}^* G_1 \begin{pmatrix} v_i \\ w_i \end{pmatrix}^{*\prime} & \\ & & G_2 \end{pmatrix} \quad (i = 1, 2).$$

根据第十章定理 1.4(Witt 定理的推广), 推出

$$\begin{pmatrix} \begin{pmatrix} v_1 \\ w_1 \end{pmatrix}^* G_1 \begin{pmatrix} v_1 \\ w_1 \end{pmatrix}^{*\prime} & \\ & G_2 \end{pmatrix}$$

和

$$\begin{pmatrix} \begin{pmatrix} v_2 \\ w_2 \end{pmatrix}^* G_1 \begin{pmatrix} v_2 \\ w_2 \end{pmatrix}^{*\prime} & \\ & G_2 \end{pmatrix}$$

合同, 即有 $(n-2)\times(n-2)$ 可逆矩阵 R 存在, 使

$$R\begin{pmatrix} \begin{pmatrix} v_1 \\ w_1 \end{pmatrix}^* G_1 \begin{pmatrix} v_1 \\ w_1 \end{pmatrix}^{*\prime} & \\ & G_2 \end{pmatrix}R'$$

$$=\begin{pmatrix} \begin{pmatrix} v_2 \\ w_2 \end{pmatrix}^* G_1 \begin{pmatrix} v_2 \\ w_2 \end{pmatrix}^{*\prime} & \\ & G_2 \end{pmatrix}.$$

因之

$$\begin{pmatrix} v_2 & x_2 \\ w_2 & y_2 \\ \begin{pmatrix} v_1 \\ w_1 \end{pmatrix}^* & \\ & I \end{pmatrix}^{-1} \begin{pmatrix} I & \\ & R \end{pmatrix} \begin{pmatrix} v_1 & x_1 \\ w_1 & y_1 \\ \begin{pmatrix} v_1 \\ w_1 \end{pmatrix}^* & \\ & I \end{pmatrix} = \begin{pmatrix} A & B \\ 0 & I \end{pmatrix},$$

而 $AG_1A' + G_1 \equiv BG_2B'$. 于是

$$\begin{pmatrix} v_1 \\ w_1 \end{pmatrix} = \begin{pmatrix} v_2 \\ w_2 \end{pmatrix} A,$$

而 $A \in O_n(F, G)$. 因此定理这时也成立.

§3 $O_n(F,G)$ 中元素的形式

先研究 $p = \nu$ 的情形. 设

$$G_1 = \begin{pmatrix} 0 & I^{(p)} \\ 0 & 0 \end{pmatrix},$$

于是

$$G_1 + G_1' = \begin{pmatrix} 0 & I \\ I & 0 \end{pmatrix}.$$

那么

$$T=\begin{pmatrix} A & B \\ C & D \end{pmatrix}\in O_n(F,G)$$

当且仅当

$$TG_1T'+G_1=\begin{pmatrix} AB' & AD'+BC'+I \\ & CD' \end{pmatrix}$$

与一个对角元素属于 $\mathfrak{M}$ 的对角矩阵合同, 即 AB', CD' 是对角元素属于 $\mathfrak{M}$ 的对称矩阵而 $AD'+BC'=I$.

从 $TG_1T'+G_1$ 与一个对角元素属于 $\mathfrak{M}$ 的对角矩阵合同我们推出, $T^{-1}G_1T^{-1'}+G$ 亦然. 但

$$T^{-1}=\begin{pmatrix} D' & B' \\ C' & A' \end{pmatrix},$$

所以 $D'B, C'Ar$ 是对角元素属于 $\mathfrak{M}$ 的对称矩阵而

$$D'A+B'C=I.$$

定理 1 设 $\nu=p$. 以下这些元素属于 $O_n(F,G)$:

I. $\begin{pmatrix} I & K \\ 0 & I \end{pmatrix}$ (K 是对角元素属于 $\mathfrak{M}$ 的对称矩阵);

II. $\begin{pmatrix} A & 0 \\ 0 & A'^{-1} \end{pmatrix}$ (A 可逆);

III. $\begin{pmatrix} J & I+J \\ I+J & J \end{pmatrix}$ ($J^2=J$ 是对角矩阵).

更进一步, $O_n(F,G)$ 中任一元素皆可表示成形状

$$\begin{pmatrix} I & \\ X & I \end{pmatrix}\begin{pmatrix} A & \\ & A'^{-1} \end{pmatrix}\begin{pmatrix} I & Y \\ & I \end{pmatrix}\begin{pmatrix} J & I+J \\ I+J & J \end{pmatrix},$$

其中 X, Y 是对角元素与属于 $\mathfrak{M}$ 的对称矩阵, A 可逆, $J^2=J$ 是对角矩阵.

可仿第七章 §7 证之, 亦可与第九章定理 1.2, 第十章定理 4.1 相比较.

现在研究 $\nu<p$ 的情形. 设

$$G_1=\begin{pmatrix} 0 & I^{(\nu)} & \\ 0 & 0 & \\ & & \Delta \end{pmatrix},$$

而

$$\Delta=\begin{pmatrix}[\alpha_1,\cdots,\alpha_{p-\nu}] & I\\ 0 & [\beta_1,\cdots,\beta_{p-\nu}]\end{pmatrix}$$

是定号的.

定理 2　设 $\nu<p$. 以下这些矩阵属于 $O_n(F,G)$:

I. $\begin{pmatrix}A & B & \\ C & D & \\ & & I\end{pmatrix}$, 而 $\begin{pmatrix}A & B\\ C & D\end{pmatrix}\in O_{2\nu+d}\left(F,\begin{pmatrix}0 & I^{(\nu)} & \\ 0 & 0 & \\ & & G_2\end{pmatrix}\right)$;

II. $\begin{pmatrix}I & P\Delta P' & P\\ & I & \\ & (\Delta+\Delta')P' & I\end{pmatrix}$, $\begin{pmatrix} & I & & \\ & P\Delta P' & I & P\\ & (\Delta+\Delta')P & & I\end{pmatrix}$,

其中 P 为任意 $\nu\times(2p-2\nu)$ 矩阵;

III. $\begin{pmatrix}I & & \\ & I & \\ & & U\end{pmatrix}$, 而 $U\in O_{n-2\nu}\left(F,\begin{pmatrix}\Delta & \\ & G_2\end{pmatrix}\right)$.

更进一步, $O_n(F,G)$ 中任一元素皆可表作

$$\begin{pmatrix}I & & \\ X\Delta X' & I & X\\ (\Delta+\Delta')X' & & I\end{pmatrix}\begin{pmatrix}A & B & \\ C & D & \\ & & U\end{pmatrix}\begin{pmatrix}I & Y\Delta Y' & Y\\ & I & \\ & (\Delta+\Delta')Y' & I\end{pmatrix}\begin{pmatrix}J & I+J & \\ I+J & J & \\ & & I\end{pmatrix}.$$

可仿第七章 §8 证之, 亦可与第九章定理 1.3, 第十章定理 4.2 相比较.

§4　正 交 平 延

以下总以 S 表示交错矩阵 G_1+G_1'.

定理 1　辛平延 $I+\lambda Sv'v$ 是正交矩阵当且仅当 $\lambda+\lambda^2vG_1v'\in\mathfrak{M}$.

【证】　我们有

$$\begin{aligned}&(I+\lambda Sv'v)G_1(I+\lambda Sv'v)'+G_1\\ =&\lambda Sv'vG_1+\lambda G_1v'vS+\lambda^2Sv'vG_1v'vS\\ \equiv&(\lambda+\lambda^2vG_1v')Sv'vS.\end{aligned}$$

因 $Sv'vS$ 是对角元素为 F^2 中元素的对称矩阵, 故 $I+\lambda Sv'v\in O_n(F,G)$ 当且仅当 $\lambda+\lambda^2vG_1v'\in\mathfrak{M}$.

定义 1　正交平延 $I+\lambda Sv'v$, 其中 $\lambda+\lambda^2vG_1v'\in\mathfrak{M}$, 称为奇异, 半奇异或非奇异依 v 奇异, 半奇异或非奇异而定.

我们指出, 半奇异平延存在当且仅当 G 的指数 $\nu \geqslant 1$.

定理 2 设 $\nu \geqslant 1$. 每个正交平延皆正交相似于以下形状的一个平延:

$$(1)\qquad \begin{pmatrix} 1+\lambda\mu & 0 & \lambda\mu^2 & 0 & \\ 0 & I^{(\nu-1)} & 0 & 0 & \\ \lambda & 0 & 1+\lambda\mu & 0 & \\ 0 & 0 & 0 & I^{(\nu-1)} & \\ & & & & I \end{pmatrix},$$

其中 $\lambda+\lambda^2\mu \in \mathfrak{M}$.

【证】 设 $I+\lambda Sv'v$ 是正交平延. 置 $\mu = vG_1v'$, 则 $\lambda+\lambda^2\mu \in \mathfrak{M}$. 因

$$(1\ 0\ \mu\ 0\ 0)\begin{pmatrix} 0 & I & \\ 0 & 0 & \\ & & \Delta \end{pmatrix}(1\ 0\ \mu\ 0\ 0)' = \mu,$$

故依定理 2.3(如 v 奇异) 或定理 2.4(如 v 非奇异), 知有正交矩阵 T 存在, 使

$$v = (1\ 0\ \mu\ 0\ 0)T.$$

那么, $T(I+\lambda Sv'v)T^{-1}$ 即为 (1).

我们注意, 如 v 半奇异, 则为使 $I+\lambda Sv'v$ 是正交平延, 只要 $\lambda \in \mathfrak{M}$ 即可. 特别有

系理 1 设 $\nu \geqslant 1$. 任一奇异平延皆正交相似于以下形状的一个平延:

$$\begin{pmatrix} I & & & \\ \lambda & & \mathrm{I} & \\ & 0 & & \\ & & & I \end{pmatrix},$$

而 $\lambda \in \mathfrak{M}$.

我们再注意, 如 v 非奇异, 取 $\lambda = \mu^{-1}$ 就有 $\lambda+\lambda^2\mu = 0$. 因之有

系理 2 设 $\nu \geqslant 1$. $O_n(F,G)$ 中包有非奇异平延

$$\begin{pmatrix} & & \lambda^{-1} & & \\ & I & & & \\ \lambda & & & & \\ & & & I & \\ & & & & I \end{pmatrix},$$

对一切 $\lambda \in F^*$.

定理 3　群 $O_n(F,G)$ 由正交平延所演成.

【证】　以 $\mathfrak{T}$ 表由正交平延所演成的群. 我们要证明 $\mathfrak{T} = O_n(F,G)$. 分别研究以下两种情形:

(i)$\nu = p$. 设 K 为对角元素属于 $\mathfrak{M}$ 的对称矩阵, 则

$$K = K_1 + K_2 + \cdots + K_m,$$

而 $K_i = [0, \cdots, 0, k, 0, \cdots, 0], k \in \mathfrak{M}$ 或

$$K_i = \begin{pmatrix} 0 & & & \\ & 0 & a & \\ & a & 0 & \\ & & & 0 \end{pmatrix}.$$

于是

$$\begin{pmatrix} I & K \\ 0 & I \end{pmatrix} = \begin{pmatrix} I & K_1 \\ 0 & I \end{pmatrix}\begin{pmatrix} I & K_2 \\ 0 & I \end{pmatrix}\cdots\begin{pmatrix} I & K_m \\ 0 & I \end{pmatrix}.$$

显然, 如 $K_i = [0, \cdots, 0, k, 0, \cdots, 0]$, 而 $k \in \mathfrak{M}$, 则

$$\begin{pmatrix} I & K_i \\ 0 & I \end{pmatrix}$$

为正交平延. 如 $K_i = \begin{pmatrix} 0 & a \\ a & 0 \end{pmatrix}$(为书写简单起见设 $p = 2$), 则

$$\begin{pmatrix} \begin{pmatrix} 1 & \\ k^{-1}a & 1 \end{pmatrix} & \\ & \begin{pmatrix} 1 & k^{-1}a \\ & 1 \end{pmatrix} \end{pmatrix}\begin{pmatrix} \mathrm{I} & \begin{matrix} k & 0 \\ 0 & 0 \end{matrix} \\ & I \end{pmatrix}$$

$$\cdot\begin{pmatrix} 1 & K_i \\ & I \end{pmatrix}\begin{pmatrix} \begin{pmatrix} 1 & \\ k^{-1}a & 1 \end{pmatrix} & \\ & \begin{pmatrix} 1 & k^{-1}a \\ & 1 \end{pmatrix} \end{pmatrix}^{-1}$$

$$= \begin{pmatrix} I & \begin{matrix} k & \\ & k^{-1}a^2 \end{matrix} \\ & I \end{pmatrix} = \begin{pmatrix} \mathrm{I} & \begin{matrix} k & 0 \\ 0 & 0 \end{matrix} \\ & I \end{pmatrix}\begin{pmatrix} I & \begin{matrix} 0 & \\ & k^{-1}a^2 \end{matrix} \\ & I \end{pmatrix} \quad (k \in \mathfrak{M}),$$

因此

$$\begin{pmatrix} I & K_i \\ 0 & I \end{pmatrix}$$

为正交平延之积. 这就证明了

$$(2)\qquad \begin{pmatrix} I & K \\ 0 & I \end{pmatrix} \ (K\ 为对角元素属于\ \mathfrak{M}\ 的对称矩阵)$$

属于 $\mathfrak{T}$.

其次,$\mathfrak{T}$ 包有

$$\begin{pmatrix} & & \lambda^{-1} & \\ & I & & \\ \lambda & & & \\ & & & I \end{pmatrix}\begin{pmatrix} & & I & \\ & I & & \\ 1 & & & \\ & & & 1 \end{pmatrix}=\begin{pmatrix} \lambda^{-1} & & & \\ & I & & \\ & & \lambda & \\ & & & I \end{pmatrix}$$

以及

$$\begin{pmatrix} 1 & \lambda & & & & \\ & 1 & & & & \\ & & I & & & \\ & & & 1 & & \\ & & & \lambda & 1 & \\ & & & & & I \end{pmatrix}=\begin{pmatrix} 1 & & & & & \\ & 0 & & & 1 & \\ & & I & & & \\ & & & 1 & & \\ & 1 & & & 0 & \\ & & & & & I \end{pmatrix}.$$

$$\begin{pmatrix} 1 & & \lambda & & & \\ & 1 & & \lambda & & \\ & & I & & & \\ & & & 1 & & \\ & & & & 1 & \\ & & & & & I \end{pmatrix}\begin{pmatrix} 1 & & & & & \\ & 0 & & & 1 & \\ & & I & & & \\ & & & 1 & & \\ & 1 & & & 0 & \\ & & & & & I \end{pmatrix}^{-1}$$

对所有 $\lambda \in F^*$. 因 $GL_\nu(F)$ 由 $[\lambda, 1, \cdots, 1]$ 及 $B_{ij}(\lambda)$ 所生成, 而 $B_{ij}(\lambda)$ 在 $GL_\nu(F)$ 中互相共轭, 故 $\mathfrak{T}$ 包有

$$(3)\qquad \begin{pmatrix} A & 0 \\ 0 & A'^{-1} \end{pmatrix},$$

对一切可逆 A.

最后, 因

$$\begin{pmatrix} & & 1 & \\ & 1 & & \\ 1 & & & \\ & & & 1 \end{pmatrix}\begin{pmatrix} 1 & & & \\ & & & 1 \\ & & 1 & \\ & 1 & & \end{pmatrix}=\begin{pmatrix} 0 & I \\ I & 0 \end{pmatrix},$$

$\mathfrak{T}$ 包有所有

(4) $$\begin{pmatrix} J & I+J \\ I+J & J \end{pmatrix},$$

而 $J^2 = J$ 为对角矩阵.

这样一来, 因 $O_n(F,G)$ 由一切形为 (2), (3), (4) 的元素所生成, 故 $\mathfrak{T} = O_n(F,G)$.

(ii) $\nu < p$. 依定理 3.2, 只需证

$$\begin{pmatrix} A & B & \\ C & D & \\ & & I \end{pmatrix}, \begin{pmatrix} I & & \\ & I & \\ & & U \end{pmatrix} \text{ 及 } \begin{pmatrix} I & P\Delta P' & P \\ & I & \\ & \Delta+\Delta'P' & I \end{pmatrix}$$

都属于 $\mathfrak{T}$. 由 (i) 知

$$\begin{pmatrix} A & B & \\ C & D & \\ & & I \end{pmatrix} \in \mathfrak{T},$$

而

$$\begin{pmatrix} I & P\Delta P' & P \\ & I & \\ & (\Delta+\Delta')P' & I \end{pmatrix} \in \mathfrak{T}$$

的证明与第十章定理 5.3 中的证明相似, 因而略去. 关于

$$\begin{pmatrix} I & & \\ & I & \\ & & U \end{pmatrix} \in \mathfrak{T}$$

的证明我们叙述成:

引理 设 Δ 为无亏数的正则定号矩阵, 而 $\begin{pmatrix} \Delta & \\ & G_2 \end{pmatrix}$ 是指数 0 的正则矩阵, 则 $O_n\left(F, \begin{pmatrix} \Delta & \\ & G_2 \end{pmatrix}\right)$ 中任一元素皆正交平延之积.

【证】 因 Δ 定号, 所有向量皆非奇异.

设 U 是一个 $\neq I$ 的正交矩阵. 于是有一个向量 x 存在, 使 $xU \neq x$. 于是

$$\begin{aligned} 0 &\neq (x+xU)\Delta(x+xU)' \\ &= x(\Delta + U\Delta U')x' + xS(xU)', \end{aligned}$$

因 $\begin{pmatrix} \Delta & \\ & G_2 \end{pmatrix}$ 的指数为 $0, xS(xU)' = 0$; 否则将有一 d 维向量 $y \neq 0$, 使

$$0 \neq (x+xU)\Delta(x+xU)' = yG_2y'.$$

于是 $(x+xU,y)$ 将是对于 $\begin{pmatrix} \Delta & \\ & G_2 \end{pmatrix}$ 的一个奇异向量. 考查正交平延

$$T = I + \lambda S(x+xU)'(x+xU),$$

其中 $\lambda = [(x+xU)\Delta(x+xU)' + x(\Delta + U\Delta U')x'] - 1$. 于是

$$xT = xU,$$

即 $U_1 = UT$ 将 x 保持不变.

存在着一个向量 y, 使 $xSy' \neq 0$. 如 $yU_1 = y$, 令 $U_2 = U_1$; 如 $yU_1 \neq y$, 则正交平延

$$T_1 = I + \lambda S(y+yU_1)'(y+yU_1),$$

其中 $\lambda = [(y+yU_1)\Delta(y+yU_1)' + y(\Delta + U_1\Delta U_1)y']^{-1}$, 将 x 不变而将 y 变到 yU_1, 这时令 $U_2 = U_1T_1$. 于是在这两种情形都有

$$xU_2 = x,\ yU_2 = y.$$

平面 $\begin{pmatrix} x \\ y \end{pmatrix}$ 是非迷向的, 于是 $\begin{pmatrix} x \\ y \end{pmatrix}$ 也是非迷向的. 对于一组由 x, y 及 $\begin{pmatrix} x \\ y \end{pmatrix}^*$ 中向量组成的基, U_2 有形状

$$\begin{pmatrix} I^{(2)} & 0 \\ 0 & U_3 \end{pmatrix}.$$

将同样讨论应用于 U_3 并继续进行下去, 即可证得本引理.

§5 由半奇异平延所演成的群

以 $\mathfrak{F}$ 表由 $O_n(F,G)$ 中半奇异平延所演成的群. 因正交矩阵将半奇异向量仍变到半奇异向量, 故 $\mathfrak{F}$ 为 $O_n(F,G)$ 的正规子群.

定理 1 以下这些元素都是 $\mathfrak{F}$ 中的元素:

I. $\begin{pmatrix} I & K & \\ 0 & I & \\ & & I \end{pmatrix}$ (K 是对角元素属于 $\mathfrak{M}$ 的对称矩阵);

II. $\begin{pmatrix} A & & \\ & A'^{-1} & \\ & & I \end{pmatrix}$ $(A \in SL_\nu(F))$;

$$\text{III.}\ \begin{pmatrix} I+J & J & \\ J & I+J & \\ & & I \end{pmatrix}\quad (J^2=J\ \text{是偶秩的对角矩阵});$$

$$\text{IV.}\ \begin{pmatrix} I & P\Delta P' & P \\ & I & \\ & (\Delta+\Delta')P' & I \end{pmatrix}\quad (P\ \text{是任意}\ \nu\times(2p-2\nu)\ \text{矩阵}).$$

【证】 完全和定理 4.3 的证明中一样, 可以证明 I 和 II 属于 $\mathfrak{F}$.

设 $K=\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$, 则

$$\begin{pmatrix} I & K \\ & I \end{pmatrix}\begin{pmatrix} I & \\ K & I \end{pmatrix}\begin{pmatrix} I & K \\ & I \end{pmatrix}\begin{pmatrix} K & \\ & K \end{pmatrix}=\begin{pmatrix} 0 & I \\ I & 0 \end{pmatrix},$$

由此推出 III 属于 $\mathfrak{F}$.

至于Ⅳ属于 $\mathfrak{F}$ 的证明可仿第九章定理 2.2 的证明证之.

定理 2　设 $\nu\geqslant 1$. $\mathfrak{F}$ 的中心仅由单位元素组成.

【证】 设

$$\begin{bmatrix} A & B & P \\ C & D & Q \\ R & T & U \end{bmatrix}$$

是 $\mathfrak{F}$ 的一个中心元素. 因为它与一切

$$\begin{bmatrix} A_1 & & \\ & A_1'^{-1} & \\ & & I \end{bmatrix}.\quad (A_1\in SL_\nu(F))$$

交换, 故它的形状是

$$\begin{pmatrix} aI & & \\ & a^{-1}I & \\ & & U \end{pmatrix}.$$

又因它与一切

$$\begin{pmatrix} I & K & \\ & I & \\ & & I \end{pmatrix}$$

交换, 其中 K 是对角元素属于 $\mathfrak{M}$ 的对称矩阵, 故

$$a=a^{-1}=1.$$

最后, 因它与一切

$$\begin{pmatrix} I & P\Delta P' & P \\ & I & \\ & (\Delta+\Delta')P' & I \end{pmatrix}$$

交换, 故 $U=I$. 这样, 只有单位矩阵是 $\mathfrak{F}$ 的中心元素.

记 $O_n(F,G)$ 的换位子群为 $\Omega_n(F,G)$.

定理 3 设 $\nu \geqslant 1$. 群 $\Omega_n(F,G)$ 与由半奇异平延所演成的群相重.

【证】 先证 $\mathfrak{F} \subset \Omega_n(F,G)$. 因为任一半奇异向量可经一正交变换变到预先指定的任一半奇异向量, 所以半奇异平延在 $O_n(F,G)$ 中共轭于具预先指定的任一半奇异向量的半奇异平延. 因此只要证明

$$\begin{pmatrix} 1 & \lambda \\ 0 & 1 \end{pmatrix}$$

(为书写方便, 设 $p=\nu=1$), 当 λ 跑过 $\mathfrak{M}$ 时, 皆属于 $\Omega_n(F,G)$. 可写

$$\lambda = k^2(k^{-2}\lambda),$$

而 $k^2\lambda \in \mathfrak{M}, k\neq 1, k\in F$. 于是

$$\begin{pmatrix} 1 & \lambda \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} 1+k & \\ & (1+k)^{-1} \end{pmatrix}\begin{pmatrix} 1 & k^{-2}\lambda \\ & 1 \end{pmatrix}\cdot \begin{pmatrix} 1+k & \\ & (1+k)^{-1} \end{pmatrix}^{-1}\begin{pmatrix} 1 & k^{-2}\lambda \\ & 1 \end{pmatrix}^{-1}$$

为换位子, 因此 $\mathfrak{F} \subset \Omega_n(F,G)$.

其次再证 $\Omega_n(F,G) \subset \mathfrak{F}$. 这只要证, 对任意 $P,Q \in O_n(F,G), P^{-1}Q^{-1}PQ \in \mathfrak{F}$ 即可. 先证 $P^{-1}Q^{-1}PQ \in \mathfrak{F}$, 对任意 $P \in O_n(F,G)$ 及任意正交平延 Q. 依定理 4.2, 有一正交矩阵 T 存在, 使得

$$TQT^{-1} = \begin{pmatrix} 1+\lambda\mu & & \lambda\mu^2 & & \\ & I & & & \\ \lambda & & 1+\lambda\mu & & \\ & & & I & \\ & & & & I \end{pmatrix}, \tag{1}$$

而 $\lambda+\lambda^2\mu \in \mathfrak{M}$. 因 $\mathfrak{F}$ 是 $O_n(F,G)$ 的正规子群, 故由 $T(P^{-1}Q^{-1}PQ)T \in \mathfrak{F}$ 可得

$P^{-1}Q^{-1}PQ \in \mathfrak{F}$. 因此不失普遍性, 可设 Q 即为 (1). 依定理 3.2, P 可表作

$$P = \begin{pmatrix} I & & \\ X\Delta X' & I & X \\ (\Delta+\Delta')X' & & I \end{pmatrix}\begin{pmatrix} A & B & \\ C & D & \\ & & U \end{pmatrix}\begin{pmatrix} I & Y\Delta Y' & Y \\ & I & \\ & (\Delta+\Delta')Y' & I \end{pmatrix}\begin{pmatrix} I+J & J & \\ J & I+J & \\ & & I \end{pmatrix}.$$

再依定理 1, P 可表作

$$P = \begin{pmatrix} a & & & & \\ & I & & & \\ & & a^{-1} & & \\ & & & I & \\ & & & & U \end{pmatrix} P_1 \text{ 或 } \begin{pmatrix} 0 & & a^{-1} & & \\ & I & & & \\ a & & 0 & & \\ & & & I & \\ & & & & U \end{pmatrix} P_1,$$

而 $P_1 \in \mathfrak{F}$. 因此只需研究

$$C_1 = \begin{pmatrix} a & \\ & a^{-1} \end{pmatrix}^{-1}\begin{pmatrix} 1+\lambda\mu & \lambda\mu^2 \\ \lambda & 1+\lambda\mu \end{pmatrix}^{-1}\begin{pmatrix} a & \\ & a^{-1} \end{pmatrix}\begin{pmatrix} 1+\lambda\mu & \lambda\mu^2 \\ \lambda & 1+\lambda\mu \end{pmatrix}$$

及

$$C_2 = \begin{pmatrix} & a^{-1} \\ a & \end{pmatrix}^{-1}\begin{pmatrix} 1+\lambda\mu & \lambda\mu^2 \\ \lambda & 1+\lambda\mu \end{pmatrix}^{-1}\begin{pmatrix} & a^{-1} \\ a & \end{pmatrix}\begin{pmatrix} 1+\lambda\mu & \lambda\mu^2 \\ \lambda & 1+\lambda\mu \end{pmatrix}$$

(为书写简单计, 设 $p=\nu=1$.) 我们有

$$C_1 = \begin{pmatrix} 1+(1+a^{-2})\lambda^2\mu^2 & (1+\lambda\mu)(1+a^{-2})\lambda\mu^2 \\ (1+\lambda\mu)(1+a^2)\lambda & 1+(1+a^2)\lambda^2\mu^2 \end{pmatrix}$$

及

$$C_2 = \begin{pmatrix} a^{-2}\lambda^2+(1+\lambda\mu)^2 & (1+\lambda\mu)(a^{-2}\lambda+\lambda\mu^2) \\ (1+\lambda\mu)(\lambda a^2\lambda\mu^2) & (1+\lambda\mu)^2+a^2\lambda^2\mu^4 \end{pmatrix},$$

于是

$$C_1\mathfrak{F} = \begin{cases} \begin{pmatrix} [1+(1+a^{-1})\lambda\mu]^2 & \\ & [1+(1+a^{-1})\lambda\mu]^{-2} \end{pmatrix}\mathfrak{F}, \\ \qquad \text{如} 1+(1+a^{-1})\lambda\mu \neq 0, \\ \begin{pmatrix} [1+(1+a)\lambda\mu]^{-2} & \\ & [1+(1+a)\lambda\mu]^2 \end{pmatrix}\mathfrak{F}, \\ \qquad \text{如} 1+(1+a)\lambda\mu \neq 0 \end{cases}$$

及

$$C_2\mathfrak{F} = \begin{cases} \begin{pmatrix} [a^{-1}\lambda + (1+\lambda\mu)]^2 & \\ & [a^{-1}\lambda + (1+\lambda\mu)]^{-2} \end{pmatrix}\mathfrak{F}, \\ \qquad \text{如} a^{-1}\lambda + (1+\lambda\mu) \neq 0 \\ \begin{pmatrix} [(1+\lambda\mu) + a\lambda\mu^2]^{-2} & \\ & [(1+\lambda\mu) + a\lambda\mu^2]^2 \end{pmatrix}\mathfrak{F}, \\ \qquad \text{如} (1+\lambda\mu) + a\lambda\mu^2 \neq 0. \end{cases}$$

因此 $P^{-1}Q^{-1}PQ \in \mathfrak{F}$.

现在设 P 和 Q 是 $O_n(F,G)$ 中任意两元素. 依定理 4.3, Q 可写成正交平延之积. 设 Q 是 n 个正交平延之积, 我们对 n 行施归纳法. 我们可以写 $Q = Q_1Q_2$, 其中 Q_1 是正交平延而 Q_2 是 $n-1$ 个正交平延之积, 于是

$$\begin{aligned} P^{-1}Q^{-1}PQ &= P^{-1}Q_2^{-1}Q_1^{-1}PQ_1Q_2 \\ &= (P^{-1}Q_2^{-1}PQ_2)Q_2^{-1}(P^{-1}Q_1^{-1}PQ_1)Q_2, \end{aligned}$$

依归纳法假设,

$$P^{-1}Q_2^{-1}PQ_2 \in \mathfrak{F} \text{ 及 } P^{-1}Q_1^{-1}PQ_1 \in \mathfrak{F},$$

因此

$$P^{-1}Q^{-1}PQ \in \mathfrak{F}.$$

定理 3 至此完全证毕.

定理 4 设 $\nu \geqslant 1$, 则任一半奇异平延在 $\Omega_n(F,G)$ 之中皆共轭于具奇异向量 $(1,0,\cdots,0)$ 的奇异平延, 即皆共轭于以下形状的一个平延:

$$\begin{pmatrix} & I & & \\ \lambda & & & \\ & 0 & I & \\ & & & I \end{pmatrix},$$

其中 $\lambda \in \mathfrak{M}$.

【证】 设 $T = I + \lambda S v' v$ 是一个半奇异平延, v 为半奇异向量. 依定理 2.3 的系理, 有正交矩阵 A, 使

$$(1,0,\cdots,0) = vA.$$

依定理 1 和定理 3 知, 可以写

$$A = A_1 \begin{pmatrix} I & & & & \\ & a & & & \\ & & I & & \\ & & & a^{-1} & \\ & & & & U \end{pmatrix} \text{ 或 } A_1 \begin{pmatrix} I & & & & \\ & 0 & & a^{-1} & \\ & & I & & \\ & a & & 0 & \\ & & & & U \end{pmatrix},$$

而 $A_1 \in \Omega_n(F,G)$. 如后一情形出现, 则由

$$\begin{pmatrix} I & & & & \\ & 0 & & p\Delta p' & \\ & & I & & \\ & (p\Delta p')^{-1} & & 0 & \\ & & & & I+S(p\Delta p')^{-1}P'P \end{pmatrix} \in \Omega_n(F,G)$$

也可以写

$$A = A_1 \begin{pmatrix} I & & & & \\ & a & & & \\ & & I & & \\ & & & a^{-1} & \\ & & & & U \end{pmatrix},$$

而 $A_1 \in \Omega_n(F,G)$. 于是

$$A_1^{-1}TA_1 = \begin{pmatrix} I & & & & \\ & a & & & \\ & & I & & \\ & & & a^{-1} & \\ & & & & U \end{pmatrix} A^{-1}TA \begin{pmatrix} I & & & & \\ & a & & & \\ & & I & & \\ & & & a^{-1} & \\ & & & & U \end{pmatrix}^{-1}$$

$$= \begin{pmatrix} I & & & & \\ & a & & & \\ & & I & & \\ & & & a^{-1} & \\ & & & & U \end{pmatrix} [I+\lambda S(1,0\cdots0)'(1,0\cdots0)] \begin{pmatrix} I & & & & \\ & a^{-1} & & & \\ & & I & & \\ & & & a & \\ & & & & U \end{pmatrix}$$

$$= \begin{cases} \begin{pmatrix} & I & & & \\ \lambda & & & & \\ & & & I & \\ & & 0 & & \\ & & & & I \end{pmatrix} & (\text{如}\nu \geqslant 2), \\ \begin{pmatrix} & I & & & \\ a^{-2}\lambda & & & & \\ & & & I & \\ & & 0 & & \\ & & & & I \end{pmatrix} & (\text{如}\nu = 1). \end{cases}$$

因此定理 4 得证.

系理 设 $\nu \geqslant 1$, 则任一半奇异平延在 $\Omega_n(F,G)$ 中皆共轭于一个具预先给定的半奇异向量的半奇异平延.

§6 $\Omega_n(F,G)$ 的单性

定理 1 设 $\nu \geqslant 1$, 则 $\Omega_n(F,G)$ 是单群.

先证次之引理.

引理 1 设 $\mathfrak{N}$ 是 $\Omega_n(F,G)$ 的一个正规子群, 如果 $\mathfrak{N}$ 包有一个半奇异平延, 则 $\mathfrak{N}=\Omega_n(F,G)$.

【证】 设 $\mathfrak{N}$ 包有一个半奇异平延. 依定理 5.4, 可设 $\mathfrak{N}$ 包有以下形状的一个奇异平延:

(1)

$$\begin{pmatrix} & I & & & \\ \lambda & & & & \\ & & & I & \\ & & 0 & & \\ & & & & I \end{pmatrix},$$

而 $\lambda \in \mathfrak{M}$. 如果我们能够证明 $\mathfrak{N}$ 包有一切形状 (1) 的奇异平延, 则本引理即从定理 5.4 推出.

首先, 我们断言 $\mathfrak{N}$ 包有一个形如 (1) 的元素而 $\lambda \neq 1$. 因为, 如 $\lambda=1$, 可以 F 中选一元素 $a \neq 0,1$, 于是从

$$\begin{pmatrix} a^2 & \\ & a^{-2} \end{pmatrix}^{-1}\begin{pmatrix} 1 & \\ 1 & 1 \end{pmatrix}^{-1}\begin{pmatrix} a^2 & \\ & a^{-2} \end{pmatrix}\begin{pmatrix} 1 & \\ 1 & 1 \end{pmatrix}=\begin{pmatrix} 1 & \\ (a^4+1) & 1 \end{pmatrix},$$

而 $a^4+1 \neq 0$, 推出我们的断言.

为书写简便起见, 设 $p=\nu=1$. 于是 $\mathfrak{N}$ 包有

$$\begin{pmatrix} 1 & \lambda^{-1} \\ & 1 \end{pmatrix}\begin{pmatrix} 1 & \\ \lambda & 1 \end{pmatrix}\begin{pmatrix} 1 & \lambda^{-1} \\ & 1 \end{pmatrix}^{-1}=\begin{pmatrix} 0 & \lambda^{-1} \\ \lambda & 0 \end{pmatrix}$$

及

$$\begin{pmatrix} a^2 & \\ & a^{-2} \end{pmatrix}^{-1}\begin{pmatrix} & \lambda^{-1} \\ \lambda & \end{pmatrix}\begin{pmatrix} a^2 & \\ & a^{-2} \end{pmatrix}=\begin{pmatrix} & a^{-4}\lambda^{-1} \\ a^4\lambda & \end{pmatrix},$$

以及

$$\begin{pmatrix} 0 & \lambda^{-1} \\ \lambda & 0 \end{pmatrix} \begin{pmatrix} & a^{-4}\lambda^{-1} \\ a^4\lambda & \end{pmatrix} = \begin{pmatrix} a^4 & \\ & a^{-4} \end{pmatrix}.$$

因 F 为无限域, 可以设 $a^4 \neq 1$. 因之 $\mathfrak{N}$ 包有

$$\begin{pmatrix} 1 & \\ \lambda & 1 \end{pmatrix} \begin{pmatrix} a^4 & \\ & a^{-4} \end{pmatrix}^{-1} \begin{pmatrix} 1 & \\ \lambda & 1 \end{pmatrix} \begin{pmatrix} a^4 & \\ & a^{-4} \end{pmatrix} = \begin{pmatrix} 1 & \\ \lambda(a^8+1) & 1 \end{pmatrix},$$

因 $a^4 \neq 1$, 故 $a^8 \neq 1$. 当 λ 跑过 $\mathfrak{M}$ 时, $\lambda(a^8+1)$ 亦然. 这就证明了 $\mathfrak{N}$ 包有一切形状 (1) 的平延. 因此 $\mathfrak{N} = \Omega_n(F,G)$.

现在来证明定理 1. 设 $\mathfrak{N}$ 是 $\Omega_n(F,G)$ 的一个正规子群, 而 $\mathfrak{N}$ 不只含单位元素. 我们要证明 $\mathfrak{N} = \Omega_n(F,G)$. 设 $\mathfrak{N} \ni N$, 而 N 不是单位矩阵. 因 $\Omega_n(F,G)$ 的中心仅由单位矩阵组成, 而 $\Omega_n(F,G)$ 由半奇异正交平延演成, 所以有一半奇异正交平延 T 存在, 使

$$T^{-1}N^{-1}TN \neq I.$$

设 T 具半奇异向量 x, 即

$$T = I + \lambda Sx'x \qquad (\lambda \in \mathfrak{M}).$$

于是

$$N^{-1}TN = I + \lambda S(xN)'xN.$$

让我们研究

$$\begin{pmatrix} x \\ xN \end{pmatrix} G_1 \begin{pmatrix} x \\ xN \end{pmatrix}' \equiv \begin{pmatrix} xG_1x' & xS(xN)' \\ & (xN)G_1(xN)' \end{pmatrix}.$$

分别考虑以下两种情形:

(i) $xS(xN)' \neq 0$. 设 $xS(xN)' = \alpha$. 因

$$\begin{pmatrix} 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & \alpha & 0 & 0 \end{pmatrix} G_1 \begin{pmatrix} 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & \alpha & 0 & 0 \end{pmatrix}' = \begin{pmatrix} 0 & \alpha \\ 0 & 0 \end{pmatrix},$$

依定理 2.5, 有正交矩阵 R 存在, 使

$$\begin{pmatrix} 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & \alpha & 0 & 0 \end{pmatrix} = \begin{pmatrix} x \\ xN \end{pmatrix} R.$$

因 $\Omega_n(F,G)$ 是 $O_n(F,G)$ 的正规子群, 从 $R^{-1}\mathfrak{N}R = \Omega_n(F,G)$ 可推出 $\mathfrak{N} = \Omega_n(F,G)$, 所以只需研究 $R^{-1}\mathfrak{N}R$ 即可. $R^{-1}\mathfrak{N}R$ 包有

$$R^{-1}(T^{-1}N^{-1}TN)R = (R^{-1}T^{-1}R)R^{-1}(N^{-1}TN)R,$$

我们有

$$R^{-1}T^{-1}R = I + \lambda S(xR)'(xR)$$
$$= I + \lambda S(1\ 0\ 0\ 0\ 0)'(1\ 0\ 0\ 0\ 0)$$
$$= \begin{pmatrix} I & & & \\ \lambda & & & \\ & 0 & \mathrm{I} & \\ & & & \\ & & & I \end{pmatrix}$$

及

$$R^{-1}(N^{-1}TN)R = I + \lambda S(xNR)'(xNR)$$
$$= I + \lambda S(0\ 0\ \alpha\ 0\ 0)'(0\ 0\ \alpha\ 0\ 0)$$
$$= \begin{pmatrix} I & \lambda\alpha^2 & & \\ & & 0 & \\ & \mathrm{I} & & \\ & & & I \end{pmatrix}.$$

于是

$$R^{-1}(T^{-1}N^{-1}TN)R = \begin{pmatrix} 1 & & \lambda\alpha^2 & & \\ & I & & & \\ \lambda & & \lambda^2\alpha^2+1 & & \\ & & & I & \\ & & & & I \end{pmatrix}.$$

为书写简单起见, 设 $p=\nu=1$, 于是

$$R^{-1}(T^{-1}N^{-1}TN)R = \begin{pmatrix} 1 & \lambda\alpha^2 \\ \lambda & \lambda^2\alpha^2+1 \end{pmatrix}.$$

那么 $R^{-1}\mathfrak{N}R$ 包有

$$\begin{pmatrix} 1 & \lambda^{-1} \\ & 1 \end{pmatrix}\begin{pmatrix} 1 & \lambda\alpha^2 \\ \lambda & \lambda^{-2}\alpha^2+1 \end{pmatrix}\begin{pmatrix} 1 & \lambda^{-1} \\ & 1 \end{pmatrix} = \begin{pmatrix} 0 & \lambda^{-1} \\ \lambda & \lambda^2\alpha^2 \end{pmatrix}$$

及

$$\begin{pmatrix} a^{-2} & \\ & a^2 \end{pmatrix}^{-1}\begin{pmatrix} 0 & \lambda^{-1} \\ \lambda & \lambda^2\alpha^2 \end{pmatrix}^{-1}\begin{pmatrix} a^{-2} & \\ & a^2 \end{pmatrix}.$$
$$\begin{pmatrix} 0 & \lambda^{-1} \\ \lambda & \lambda^2\alpha^2 \end{pmatrix} = \begin{pmatrix} a^4 & (1+a^4)\alpha^2\lambda \\ & a^{-4} \end{pmatrix}.$$

以及

$$\begin{pmatrix} 1 & \lambda \\ & 1 \end{pmatrix}\begin{pmatrix} a^4 & (1+a^4)\alpha^2\lambda \\ & a^{-4} \end{pmatrix}\begin{pmatrix} 1 & \lambda \\ & 1 \end{pmatrix}^{-1}\cdot$$

$$\cdot\begin{pmatrix} a^4 & (1+a^4)\alpha^2\lambda \\ & a^{-4} \end{pmatrix}^{-1} = \begin{pmatrix} 1 & (1+a^8)\lambda \\ & 1 \end{pmatrix}.$$

因 F 为无限域, 有 $a \neq 0, 1$, 因之 $a^8 \neq 1$. 这样我们的定理即从引理推出.

(ii) $xS(xN)' = 0$. 这时 $\nu \geqslant 2$, 为书写简单起见, 设 $\nu = 2$, 因

$$\begin{pmatrix} 1 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 \end{pmatrix}\begin{pmatrix} 0 & I & \\ 0 & 0 & \\ & & \varDelta \end{pmatrix}\begin{pmatrix} 1 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 \end{pmatrix}' \equiv \begin{pmatrix} 0 & 0 \\ & 0 \end{pmatrix},$$

仍依定理 2.5, 有正交矩阵 R 存在, 使

$$\begin{pmatrix} 1 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 \end{pmatrix} = \begin{pmatrix} x \\ xN \end{pmatrix} R.$$

像上一情形一样, $R^{-1}\mathfrak{N}R$ 包有

$$R^{-1}(T^{-1}N^{-1}TN)R = R^{-1}T^{-1}RR^{-1}(N^{-1}TN)R,$$

而

$$R^{-1}T^{-1}R = I + \lambda S(xR)'(xR) = \begin{pmatrix} I & & \\ \lambda & & \\ & 0 & \mathrm{I} \\ & & & I \end{pmatrix}$$

及

$$R^{-1}(N^{-1}TN)R = I + \lambda S(xNR)'(xNR) = \begin{pmatrix} I & & \\ 0 & & \\ & \lambda & \mathrm{I} \\ & & & I \end{pmatrix},$$

因之

$$R^{-1}(T^{-1}N^{-1}TN)R=\begin{pmatrix} & I & & & \\ \lambda & & & & \\ & & \lambda & \mathrm{I} & \\ & & & & I \end{pmatrix},$$

于是 $R^{-1}\mathfrak{N}R$ 包有

$$\begin{pmatrix} a^2 & & & & \\ & 1 & & & \\ & & a^{-2} & & \\ & & & 1 & \\ & & & & I \end{pmatrix}^{-1}\begin{pmatrix} & I & & & \\ \lambda & & & & \\ & & \lambda & \mathrm{I} & \\ & & & & I \end{pmatrix}^{-1}\begin{pmatrix} a^2 & & & & \\ & 1 & & & \\ & & a^{-2} & & \\ & & & 1 & \\ & & & & I \end{pmatrix}\cdot$$

$$\cdot\begin{pmatrix} & I & & & \\ \lambda & & & & \\ & & \lambda & \mathrm{I} & \\ & & & & I \end{pmatrix}=\begin{pmatrix} & I & & & \\ (a^2+1)\lambda & & & & \\ & & 0 & I & \\ & & & & I \end{pmatrix}.$$

因有 $a\in F$ 而 $a\neq 0,1$, 所以这时我们的定理仍可从引理推出.

定理 1 至此证毕.

第十二章　辛群的自同构

§1　以往结果提要

为了方便起见, 将以往关于辛群的结果扼要叙述如下:

设 K 为域, 其特征数任意. 设 F 为 K 上 $n \times n$ 非奇异交错矩阵. 从 F 的非奇异性推出 $n = 2\nu$ 是偶数, 而且有非奇异 $n \times n$ 矩阵 P, 使

$$PFP' = \begin{pmatrix} 0 & I^{(\nu)} \\ -I^{(\nu)} & 0 \end{pmatrix}.$$

以下我们假定

$$F = \begin{pmatrix} 0 & I^{(\nu)} \\ -I^{(\nu)} & 0 \end{pmatrix}.$$

K 上一个 $n \times n$ 矩阵 P 称为辛矩阵, 如果

$$PFP' = F.$$

所有辛矩阵组成一群, 称为域 K 上 n 级辛群, 记作 $Sp_{2\nu}(K)$.

我们知道, 有以下的辛矩阵:

I. $\begin{pmatrix} A & 0 \\ 0 & A'^{-1} \end{pmatrix}$ $\quad (A \in GL_\nu(K))$;

II. $\begin{pmatrix} I & S \\ 0 & I \end{pmatrix}, \begin{pmatrix} I & 0 \\ T & I \end{pmatrix}$ $\quad (S' = S, T' = T)$;

III. $\begin{pmatrix} J & I - J \\ -(I - J) & J \end{pmatrix}$ $\quad$ ($J^2 = J$ 为对角形矩阵).

并且还知道, 任一辛矩阵 P 皆可表作形状

$$P = \begin{pmatrix} I & \\ T & I \end{pmatrix} \begin{pmatrix} A & \\ & A'^{-1} \end{pmatrix} \begin{pmatrix} I & S \\ & I \end{pmatrix} \begin{pmatrix} J & I - J \\ -(I - J) & J \end{pmatrix},$$

其中 $T' = T$, $S' = S$, $A \in GL_\nu(K)$, 而 $J^2 = J$ 为对角形矩阵; 但上述表达式并不唯一.

一般说来,

$$P=\begin{pmatrix} A & B \\ C & D \end{pmatrix},\quad A=A^{(\nu)},\quad B=B^{(\nu)},\ \text{等等}$$

为辛矩阵, 当且仅当

$$AB'-BA'=0,\quad CD'-DC'=0,\quad AD'-BC'=I.$$

再由 P 为辛矩阵推出 P' 亦为辛矩阵, 因而也有

$$A'C-C'A=0,\quad B'D-D'B=0,\quad A'D-C'B=I.$$

$Sp_{2\nu}(K)$ 的中心仅由 $\pm I^{(2\nu)}$ 组成, $Sp_{2\nu}(K)$ 对它的中心的商群称为射影辛群, 记作 $PSp_{2\nu}(K)$. 如 K 的特征数为 2, 则

$$PSp_{2\nu}(K)=Sp_{2\nu}(K).$$

除开 $n=2$, $K=F_2$ 或 F_3 及 $n=4$, $K=F_2$ 这三个情形之外, $PSp_{2\nu}(K)$ 是单群.

§2 辛对合 (K 的特征数 $\neq 2$)

定义 1 一个辛矩阵 T 称为辛对合, 或简称对合, 如果

(1) $$T^2=I.$$

定理 1 辛矩阵

$$T=\begin{pmatrix} A & B \\ C & D \end{pmatrix}$$

是对合, 当且仅当

(2) $$\begin{pmatrix} A & B \\ C & D \end{pmatrix}=\begin{pmatrix} D' & -B' \\ -C' & A' \end{pmatrix},\quad \text{即 } TF \text{ 是斜对称的}.$$

【证】 因 T 是辛矩阵, 故

$$AB'=BA',\quad CD'=DC',\quad AD'-BC'=I.$$

因此

$$T^{-1}=\begin{pmatrix} D' & -B' \\ -C' & A' \end{pmatrix},$$

所以 T 是对合, 即 $T=T^{-1}$ 当且仅当 (2) 成立. 另外,

$$TF=\begin{pmatrix} -B & A \\ -D & C \end{pmatrix},$$

所以 T 是对合当且仅当 TF 是斜对称的.

定理 2　$Sp_{2\nu}(K)$ 中任一对合 T 皆辛相似于以下标准形:

$$\begin{pmatrix} J & 0 \\ 0 & J \end{pmatrix}, \tag{3}$$

其中 $J=[1,\cdots,1,-1,\cdots,-1]=\{p,q\}$(记号) 是由 p 个 $+1$ 和 q 个 -1 组成的对角形矩阵. 确切地说, 有 $P\in Sp_{2\nu}(K)$, 使

$$PTP^{-1}=\begin{pmatrix} J & 0 \\ 0 & J \end{pmatrix}.$$

【证】　当 $n=2$ 时, 定理显然成立. 实际上, 令

$$T=\begin{pmatrix} a & b \\ c & d \end{pmatrix}\quad (ad-bc=1),$$

则 (2) 推出

$$a=d,\quad b=-b,\quad c=-c.$$

于是 $b=c=0$, $a=d=\pm 1$. 因之

$$T=\pm I.$$

假定我们的定理对于阶数 $<2\nu$ 的辛对合是成立的, 我们来证明定理对于阶数 $n=2\nu$ 的辛对合也成立.

依定理 1, T 有形状

$$T=\begin{pmatrix} A & B \\ C & A' \end{pmatrix},$$

其中

$$\begin{cases} B'=-B,\ C'=-C,\ AB=B'A', \\ CA=A'C',\ A^2+BC=I. \end{cases} \tag{4}$$

因 B 斜对称, 故有非奇异矩阵 Q 存在, 使

$$QBQ'=\begin{pmatrix} b_1^{(r)} & 0 \\ 0 & 0 \end{pmatrix}=B_1\ (\text{设}),$$

其中 $b_1^{(r)}$ 是个非奇异的秩 r 的斜对称矩阵, $0 \leqslant r \leqslant \nu$. 于是, 在辛相似变换

$$X \to \begin{pmatrix} Q & \\ & Q'^{-1} \end{pmatrix} X \begin{pmatrix} Q & \\ & Q'^{-1} \end{pmatrix}^{-1}$$

之下, T 的 B 就变成 B_1. 我们不妨一开始就假设

$$(5) \qquad B = \begin{pmatrix} b_1^{(r)} & 0 \\ 0 & 0 \end{pmatrix}.$$

写

$$A = \begin{pmatrix} a_1^{(r)} & a_2^{(r,\nu-r)} \\ a_3^{(\nu-r,r)} & a_4^{(\nu-r)} \end{pmatrix}.$$

因 AB 对称, 有 $a_3 = 0$ 而且 $a_1 b_1$ 对称, 注意辛矩阵

$$P = \begin{pmatrix} I & \\ S & I \end{pmatrix}$$

将 T 变为

$$PTP^{-1} = \begin{pmatrix} I & 0 \\ S & I \end{pmatrix} \begin{pmatrix} A & B \\ C & A' \end{pmatrix} \begin{pmatrix} I & 0 \\ -S & I \end{pmatrix} = \begin{pmatrix} A - BS & B \\ * & * \end{pmatrix}.$$

因此, 如果我们选

$$S = \begin{pmatrix} b_1^{-1} a_1 & b_1^{-1} a_2 \\ (b_1^{-1} a_2)' & 0 \end{pmatrix},$$

则 PTP^{-1} 的 A 取以下形状:

$$(6) \qquad A = \begin{pmatrix} 0 & 0 \\ 0 & a_4^{(\nu-r)} \end{pmatrix},$$

因 (A, B) 的秩为 ν, 故 a_4 非奇异. 当然, 不失普遍性, 可以一开始就假设 A 有 (6) 的形状.

考虑到 (5) 和 (6), 从 (4) 推出 C 有形状

$$C = \begin{pmatrix} b_1^{-1} & 0 \\ 0 & b_2 \end{pmatrix}.$$

因此, 辛对合 T 辛相似于

$$(7) \qquad \begin{pmatrix} 0 & 0 & b_1 & 0 \\ 0 & a_4 & 0 & 0 \\ b_1^{-1} & 0 & 0 & 0 \\ 0 & b_2 & 0 & a_4' \end{pmatrix}.$$

注意 (7) 是两个辛对合

$$\begin{pmatrix} 0 & b_1 \\ b_1^{-1} & 0 \end{pmatrix} \text{ 和 } \begin{pmatrix} a_4 & 0 \\ b_2 & a_4' \end{pmatrix}$$

的直接和. 依归纳法假设, 知我们的定理当 $r \neq 0$ 及 $r \neq \nu$ 时成立. 同样, 如 C 的秩既不是 0 又不是 ν, 我们的定理也成立.

如果 B 和 C 的秩都是 0, 那么 $A^2 = I$. 于是有可逆阵 P 存在, 使 $PAP^{-1} = J$. 那么

$$\begin{pmatrix} P & 0 \\ 0 & P'^{-1} \end{pmatrix} \begin{pmatrix} A & 0 \\ 0 & A' \end{pmatrix} \begin{pmatrix} P & 0 \\ 0 & P'^{-1} \end{pmatrix}^{-1} = \begin{pmatrix} J & 0 \\ 0 & J \end{pmatrix}.$$

这时我们的定理也成立.

最后设 B 的秩是 ν. 这时辛矩阵

$$\begin{pmatrix} I & 0 \\ B^{-1}A & I \end{pmatrix}$$

将辛对合 T 变到

$$(8) \qquad \begin{pmatrix} I & 0 \\ B^{-1}A & I \end{pmatrix} \begin{pmatrix} A & B \\ C & A' \end{pmatrix} \begin{pmatrix} I & 0 \\ -B^{-1}A & I \end{pmatrix} = \begin{pmatrix} 0 & B \\ B^{-1} & 0 \end{pmatrix}.$$

因 B 是非奇异的而且是斜对称的, 这个情形只在 $\nu = 2\mu$ 是偶数时才会发生. 这时, 有非奇异矩阵 Q 存在, 使

$$QBQ' = \begin{pmatrix} 0 & I^{(\mu)} \\ -I^{(\mu)} & 0 \end{pmatrix}.$$

于是辛矩阵

$$\begin{pmatrix} Q & \\ & Q'^{-1} \end{pmatrix}$$

就将 (8) 变到

$$(9) \quad \begin{pmatrix} Q & \\ & Q'^{-1} \end{pmatrix} \begin{pmatrix} & B \\ B^{-1} & \end{pmatrix} \begin{pmatrix} Q & \\ & Q'^{-1} \end{pmatrix}^{-1} = \begin{pmatrix} 0 & \begin{pmatrix} 0 & I \\ -I & 0 \end{pmatrix} \\ -\begin{pmatrix} 0 & I \\ -I & 0 \end{pmatrix} & 0 \end{pmatrix}.$$

最后, 辛矩阵

$$\begin{pmatrix} 0 & 0 & I & 0 \\ 0 & I & 0 & 0 \\ -I & 0 & 0 & 0 \\ 0 & 0 & 0 & I \end{pmatrix}$$

将 (9) 变到

$$\begin{pmatrix} 0 & 0 & I & 0 \\ 0 & I & 0 & 0 \\ -I & 0 & 0 & 0 \\ 0 & 0 & 0 & I \end{pmatrix}\begin{pmatrix} 0 & 0 & 0 & I \\ 0 & 0 & -I & 0 \\ 0 & -I & 0 & 0 \\ I & 0 & 0 & 0 \end{pmatrix}\begin{pmatrix} 0 & 0 & I & 0 \\ 0 & I & 0 & 0 \\ -I & 0 & 0 & 0 \\ 0 & 0 & 0 & I \end{pmatrix}^{-1} = \begin{pmatrix} 0 & -I & & \\ -I & 0 & & \\ & & 0 & -I \\ & & -I & 0 \end{pmatrix}.$$

这就化到适才讨论过的情形去了.

因此我们的定理就完全证明.

定义 2 一个辛对合, 如与 (3) 辛相似, 就称为一个 $\{p,q\}$ 辛对合, 或简称 $\{p,q\}$ 对合.

我们进而研究互相交换的辛对合.

定理 3 任意一组两两交换的辛对合可同时辛相似于

$$\begin{pmatrix} J_i & 0 \\ 0 & J_i \end{pmatrix},$$

而 J_i 是对角形矩阵, 其对角线上都是 ± 1.

【证】 当 $\nu = 1$ 时, 定理显然成立. 现在用归纳法向 ν.

依定理 2, 可以假定, 这组辛对合中的一个已经用辛矩阵变到了

$$T_1 = \begin{pmatrix} J_1 & 0 \\ 0 & J_1 \end{pmatrix} \quad (J_1 = \{p,q\}, p>0, q>0).$$

那么与 T_1 交换的矩阵 T 必有形状

$$\begin{pmatrix} a_1^{(p)} & 0 & b_1^{(p)} & 0 \\ 0 & a_2^{(q)} & 0 & b_2^{(q)} \\ c_1^{(p)} & 0 & d_1^{(p)} & 0 \\ 0 & c_2^{(q)} & 0 & d_2^{(q)} \end{pmatrix}.$$

如果 T 是一个辛对合, 则

$$\begin{pmatrix} a_1 & b_1 \\ c_1 & d_1 \end{pmatrix} \text{和} \begin{pmatrix} a_2 & b_2 \\ c_2 & d_2 \end{pmatrix}$$

也是辛对合. 因此, 依归纳法假设, 本定理对 $n=2\nu$ 也成立.

定理 4　$Sp_{2\nu}(K)$ 中一组两两交换的辛对合顶多含 2^ν 个元素, 而且有含 2^ν个两两交换的辛对合组. 其次, $\{p,q\}$ 对合与 $\{p',q'\}$ 对合辛相似当且仅当 $p=p', q=q'$. 因此, 一组含 2^ν 个两两互换的辛对合分属于 $\nu+1$ 个共轭元素类, 由 $\{p,q\}$ 对合组成的共轭类由 $\begin{pmatrix}\nu\\p\end{pmatrix}=\begin{pmatrix}\nu\\q\end{pmatrix}$ 个两两交换的 $\{p,q\}$ 对合组成.

这是定理 3 的直接推论.

定理 5　在一个固定的体 K 上, 对于不同的 $\nu, Sp_{2\nu}(K)$ 互不同构.

这是定理 4 的直接推论, 因为同构映射将辛对合映到辛对合而且也将互相交换的对合映到互相交换的对合.

§3　$Sp_{2\nu}(K)$ 的自同构 (K 的特征数 $\neq 2$)

首先, 我们举出 $Sp_{2\nu}(K)$ 的以下几种类型的自同构:

I. 内自同构

$$X\to PXP^{-1},$$

其中 P 为辛矩阵.

II. 由域 K 的自同构所诱导出的自同构

$$X\to X^\sigma,$$

其中 σ 是 K 的自同构.

III. 半内自同构

$$X\to PXP^{-1},$$

其中 P 是广义辛矩阵, 即 P 适合条件

$$PFP'=aF,$$

其中 a 属于 K^*.

其次, 我们研究, 何时两个广义辛矩阵给出同一半内自同构. 设 P 和 Q 是两个广义辛矩阵, 并假定

$$PXP^{-1}=QXQ^{-1},$$

对一切 $X\in Sp_{2\nu}(K)$. 于是

$$(P^{-1}Q)X=X(P^{-1}Q),$$

因而有 $b \in K^*$, 使

$$P^{-1}Q = bI \text{ 或 } Q = bP.$$

反之, 如

$$PFP' = aF,$$

则

$$(bP)F(bP)' = b^2aF$$

及

$$(bP)X(bP)^{-1} = PXP^{-1},$$

对一切 $X \in Sp_{2\nu}(K)$. 因此, 两个广义辛矩阵 P 和 Q 给出同一半内自同构, 当且仅当有 $b \in K^*$, 使 $Q = bP$. 因为任一广义辛矩阵可表成

(1) $$\begin{pmatrix} I & 0 \\ 0 & aI \end{pmatrix} P,$$

其中 P 为辛矩阵而 $a \in K^*$, 所以辛群的每个半内自同构皆可看作由一个形为 (1) 的元素所诱导出来, 其中 P 为辛矩阵而 a 跑过 K^* 对 K^* 的平方元素 K^{*2} 所成之群的商群的一组完全代表系.

现在我们来陈述本节的主要定理.

定理 1 $Sp_{2\nu}(K)$ 的任一自同构皆具形状:

(2) $$X \to PX^{\sigma}P^{-1},$$

其中 σ 为 K 的自同构而 P 是广义辛矩阵.

【证】 用归纳法向 ν 来证明本定理. 当 $\nu = 1$ 时, 本定理是第二章定理 6.2. 现在假定定理对于级数 $< 2\nu$ 的辛群已经成立, 我们来证明它对于 2ν 级辛群也成立.

设 $X \to \mathscr{A}(X)$ 是 $Sp_{2\nu}(K)$ 的一个自同构. 元素

$$T = [1, \underbrace{-1, \cdots, -1}_{\nu-1 \text{ 个}}, 1, \underbrace{-1, \cdots, -1}_{\nu-1 \text{ 个}}]$$

是一个 $\{1, \nu-1\}$ 对合. 依定理 2.4, 使 $\mathscr{A}$ 承受一个内自同构之后, 可设

(3) $$\mathscr{A}(T) = \pm T.$$

研究与 $\pm T$ 可换的一切辛矩阵, 它们的形状是

$$(4)\qquad \begin{pmatrix} a & 0 & b & 0 \\ 0 & A_2 & 0 & B_2 \\ c & 0 & d & 0 \\ 0 & C_2 & 0 & D_2 \end{pmatrix}$$

其中 $a, b, c, d \in K$ 而 A_2, B_2, C_2, D_2 皆 $(\nu-1)\times(\nu-1)$ 矩阵. 形如 (4) 的辛矩阵组成一群 Σ. 注意形如 (4) 的辛矩阵可看作辛矩阵

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} \text{和} \begin{pmatrix} A_2 & B_2 \\ C_2 & D_2 \end{pmatrix}$$

的直接和. 显然, 有

$$(5)\qquad \mathscr{A}(\Sigma) = \Sigma.$$

研究由一切形状

$$(6)\qquad \begin{pmatrix} a & 0 & b & 0 \\ 0 & I & 0 & 0 \\ c & 0 & d & 0 \\ 0 & 0 & 0 & I \end{pmatrix}$$

的辛矩阵组成之群 Π_1, 以及由一切形状

$$(7)\qquad \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & A_2 & 0 & B_2 \\ 0 & 0 & 1 & 0 \\ 0 & C_2 & 0 & D_2 \end{pmatrix}$$

的辛矩阵组成之群 Π_2. 于是 $\Sigma = \Pi_1 \times \Pi_2$(直乘积). 我们断言, 使 $\mathscr{A}$ 承受一个内自同构之后, 可设

$$(8)\qquad \mathscr{A}(\Pi_1) = \Pi_1 \text{ 及 } \mathscr{A}(\Pi_2) = \Pi_2.$$

实际上, 如 K 中元素个数 > 3, 则 Π_1 和 Π_2 都是 Σ 的仅有的非中心真正规子群与它们各自的换位子群相重者, 因而在 $\mathscr{A}$ 之下不变, 或者 $\mathscr{A}$ 将它们互变. 如第一种情形发生, 断言已经成立. 如第二种情形发生, 依定理 2.5, 一定有 $\nu = 2$. 于是使 $\mathscr{A}$

承受内自同构

$$X \to \begin{pmatrix} 0 & 1 & & \\ 1 & 0 & & \\ & & 0 & 1 \\ & & 1 & 0 \end{pmatrix} X \begin{pmatrix} 0 & 1 & & \\ 1 & 0 & & \\ & & 0 & 1 \\ & & 1 & 0 \end{pmatrix}^{-1}$$

之后, (8) 就成立. 至于 $K=F_3$ 的证明则请读者自行补出. 因此 $\mathscr{A}$ 诱导出 Π_1 的一个自同构和 Π_2 的一个自同构. 因

$$\Pi_1 \approx Sp_2(K), \quad \Pi_2 \approx Sp_{2\nu-2}(K),$$

故依归纳法假设有

$$\mathscr{A}(X)=Q_1X^{\sigma_1}Q_1^{-1}, \quad X\in\Pi_1,$$

其中 σ_1 为 K 的自同构, 而

$$Q_1=\begin{pmatrix} q_{11} & 0 & q_{12} & 0 \\ 0 & I & 0 & 0 \\ q_{12} & 0 & q_{22} & 0 \\ 0 & 0 & 0 & I \end{pmatrix}\begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & I & 0 & 0 \\ 0 & 0 & a_0 & 0 \\ 0 & 0 & 0 & I \end{pmatrix},$$

$$\begin{pmatrix} q_{11} & q_{12} \\ q_{21} & q_{22} \end{pmatrix}\in Sp_2(K), \quad a_0\in K^*$$

及

$$\mathscr{A}(X)=Q_2X^{\sigma_2}Q_2^{-1}, \quad X\in\Pi_2,$$

其中 σ_2 为 K 的自同构, 而

$$Q_2=\begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & Q_{11} & 0 & Q_{12} \\ 0 & 0 & 1 & 0 \\ 0 & Q_{21} & 0 & Q_{22} \end{pmatrix}\begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & I & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & b_0I \end{pmatrix},$$

$$\begin{pmatrix} Q_{11} & Q_{12} \\ Q_{21} & Q_{22} \end{pmatrix}\in Sp_{2\nu-2}(K), \quad b_0\in K^*.$$

令

$$Q=\begin{pmatrix} q_{11} & 0 & q_{12} & 0 \\ 0 & Q_{11} & 0 & Q_{12} \\ q_{21} & 0 & q_{22} & 0 \\ 0 & Q_{21} & 0 & Q_{22} \end{pmatrix}\begin{pmatrix} I^{(\nu)} & 0 \\ 0 & b_0I^{(\nu)} \end{pmatrix},$$

则 Q 为广义辛矩阵, 而使 $\mathscr{A}$ 承受内自同构

$$X \to (Q^{-1}XQ)^{\sigma_2^{-1}}$$

之后, 可设

$$\mathscr{A}\begin{pmatrix} a & 0 & b & 0 \\ 0 & A_2 & 0 & B_2 \\ c & 0 & d & 0 \\ 0 & C_2 & 0 & D_2 \end{pmatrix} = \begin{pmatrix} a^\tau & 0 & \rho b^\tau & 0 \\ 0 & A_2 & 0 & B_2 \\ \rho^{-1}c^\tau & 0 & d^\tau & 0 \\ 0 & C_2 & 0 & D_2 \end{pmatrix}, \tag{9}$$

其中 $\tau = \sigma_1\sigma_2^{-1}$ 及 $\rho = a_0^{-1}b_0$. 再者, 我们可设 $\rho = 1$ 或 ρ 不是一个平方元素. 实际上, 如 $\rho = s^2$, 则

$$\begin{pmatrix} s^{-1} & & & \\ & I & & \\ & & s & \\ & & & I \end{pmatrix}\begin{pmatrix} a^\tau & 0 & \rho b^\tau & 0 \\ 0 & A_2 & 0 & B_2 \\ \rho^{-1}c^\tau & 0 & d^\tau & 0 \\ 0 & C_2 & 0 & D_2 \end{pmatrix}\begin{pmatrix} s^{-1} & & & \\ & I & & \\ & & s & \\ & & & I \end{pmatrix}^{-1}$$

$$= \begin{pmatrix} a^\tau & 0 & b^\tau & 0 \\ 0 & A_2 & 0 & B_2 \\ c^\tau & 0 & d^\tau & 0 \\ 0 & C_2 & 0 & D_2 \end{pmatrix}.$$

以 $\varDelta$ 表一切形为

$$\begin{pmatrix} [I^{(\nu)}] & [a_1, \cdots, a_v] \\ & I^{(\nu)} \end{pmatrix}$$

的辛矩阵组成之群. 于是由 (9) 推出, $\mathscr{A}$ 将 $\varDelta$ 映入自身. 考虑与 $\varDelta$ 中每个元素都交换的辛矩阵, 这些矩阵组成一群 $\varOmega$. $\varOmega$ 由一切形为

$$\begin{pmatrix} E & B \\ 0 & E \end{pmatrix}$$

的元素组成, E 为对角矩阵, 主对角线上元素为 ± 1, EB' 是对称矩阵. 实际上, 从

$$\begin{pmatrix} A & B \\ C & D \end{pmatrix}\begin{pmatrix} I & [a_1, \cdots, a_\nu] \\ 0 & I \end{pmatrix} = \begin{pmatrix} I & [a_1, \cdots, a_v] \\ & I \end{pmatrix}\begin{pmatrix} A & B \\ C & D \end{pmatrix}$$

推出

$$A = A + [a_1, \cdots, a_v]C,$$
$$A[a_1, \cdots, a_v] + B = B + [a_1, \cdots, a_\nu]D.$$

由以上两式推出 $C=0$ 及 $D=A'^{-1}$. 再从

$$A[a_1,\cdots,a_\nu]A'=[a_1,\cdots,a_\nu]$$

推出 $A=[\pm1,\cdots,\pm1]$. 于是 $\mathscr{A}$ 诱导出 Ω 的一个自同构. Ω 中平方元素组成一群 Γ_1, $\mathscr{A}$ 也诱导出 Γ_1 的一个自同构, Γ_1 由一切形如

$$\begin{pmatrix} I & S \\ 0 & I \end{pmatrix} \quad (S'=S)$$

的元素组成. 于是我们有

$$\mathscr{A}\begin{pmatrix} I & S \\ 0 & I \end{pmatrix}=\begin{pmatrix} I & S^* \\ 0 & I \end{pmatrix}. \tag{10}$$

由 (9) 知

$$\mathscr{A}\begin{pmatrix} 0 & I \\ -I & 0 \end{pmatrix}=\begin{pmatrix} 0 & D \\ -D^{-1} & 0 \end{pmatrix} \quad (D=[p,1,\cdots,1]), \tag{11}$$

从 (10) 与 (11) 推出

$$\begin{aligned}\mathscr{A}\begin{pmatrix} I & 0 \\ S & I \end{pmatrix}&=\mathscr{A}\left(\begin{pmatrix} 0 & I \\ -I & 0 \end{pmatrix}\begin{pmatrix} I & -S \\ 0 & I \end{pmatrix}\begin{pmatrix} 0 & I \\ -I & 0 \end{pmatrix}\right)\\&=\begin{pmatrix} I & 0 \\ D^{-1}S^*D^{-1} & I \end{pmatrix},\end{aligned}$$

于是有

$$\mathscr{A}\begin{pmatrix} I & 0 \\ T & I \end{pmatrix}=\begin{pmatrix} I & 0 \\ T^{**} & I \end{pmatrix},$$

对一切 $T'=T$, 则 T^{**} 亦为对称. 这告诉我们 $\mathscr{A}$ 诱导出 Γ_2 的一个自同构, 而 Γ_2 由一切形为

$$\begin{pmatrix} I & 0 \\ T & I \end{pmatrix} \quad (T'=T)$$

的元素所组成.

考查 $Sp_{2\nu}(K)$ 中将 Γ_1, Γ_2 各自变到它们自身的那些元素. 它们组成一群 Λ, 由一切形为

$$\begin{pmatrix} A & 0 \\ 0 & A'^{-1} \end{pmatrix}$$

的元素组成. 我们有

$$\mathscr{A}\begin{pmatrix} A & 0 \\ 0 & A'^{-1} \end{pmatrix} = \begin{pmatrix} A^{\dagger} & 0 \\ 0 & (A^{\dagger})'^{-1} \end{pmatrix}$$

考查 Λ 中

$$T_{12}(\lambda) = \begin{pmatrix} 1 & \lambda & & & & \\ 0 & 1 & & & & \\ & & I^{(\nu-2)} & & & \\ & & & 1 & 0 & \\ & & & -\lambda & 1 & \\ & & & & & I^{(\nu-2)} \end{pmatrix}$$

在 $\mathscr{A}$ 之下的像. 因 T_{12} 与一切形为

$$\begin{pmatrix} I^{(2)} & & & \\ & I^{(\nu-2)} & & \\ & & I^{(2)} & \\ & & & A^{(\nu-2)'-1} \end{pmatrix} \quad (A^{(\nu-2)} \in GL_{\nu-2}(K))$$

的元素皆可换, 亦与一切形为

$$\begin{pmatrix} I^{(v)} & \nu & 0 \\ & 0 & 0^{(\nu-1)} \\ & & I^{(\nu)} \end{pmatrix}$$

的元素皆可换, 故

$$\mathscr{A}(T_{12}(\lambda)) = \begin{pmatrix} \begin{pmatrix} a & b \\ 0 & d \end{pmatrix} & & & \\ & I^{(\nu-2)} & & \\ & & \begin{pmatrix} a & b \\ 0 & d \end{pmatrix}'^{-1} & \\ & & & I^{(\nu-2)} \end{pmatrix}$$

令

$$T_2 = [1, \underbrace{-1, \cdots, -1}_{\nu-2\text{个}}, 1, \underbrace{-1, \cdots, -1}_{\nu-2\text{个}}]$$

则 $(T_{12}(\lambda)T_2)^2 = I$. 又从 (9) 有 $\mathscr{A}(T_2) = T_2$, 故有

$$\begin{pmatrix} a & -b \\ & -d \end{pmatrix}^2 = I.$$

于是 $a = d = \pm 1$. 于是 $(T_{12}(\lambda))^2$ 在 $\mathscr{A}$ 之下的像必为形状

$$\mathscr{A}(T_{12}(\lambda)^2) = T_{12}(\mu).$$

注意 $T_{12}(1) = T_{12}\left(\frac{1}{2}\right)^2$, 故有

$$\mathscr{A}(T_{12}(1)) = T_{12}(t) \quad (t \in K^*).$$

同理, 设

$$T_{21}(\lambda) = \begin{pmatrix} 1 & 0 & & & & \\ \lambda & 1 & & & & \\ & & I^{(\nu-2)} & & & \\ & & & 1 & -\lambda & \\ & & & 0 & 1 & \\ & & & & & I^{(\nu-2)} \end{pmatrix}$$

则有

$$\mathscr{A}(T_{21}(-1)) = T_{21}(s) \quad (s \in K^*).$$

再从

$$\left[\begin{pmatrix} 1 & 1 \\ & 1 \end{pmatrix}\begin{pmatrix} 1 & \\ -1 & 1 \end{pmatrix}\right]^3 = -I$$

推出

$$\left[\begin{pmatrix} 1 & t \\ & 1 \end{pmatrix}\begin{pmatrix} 1 & \\ s & 1 \end{pmatrix}\right]^3 = -I,$$

于是 $st = -1$. 那么使 $\mathscr{A}$ 承受内自同构

$$X \to \begin{pmatrix} t^{-1} & & & \\ & I^{(\nu-1)} & & \\ & & t & \\ & & & I^{(\nu-1)} \end{pmatrix} X \begin{pmatrix} t^{-1} & & & \\ & I^{(\nu-1)} & & \\ & & t & \\ & & & I^{(\nu-1)} \end{pmatrix}^{-1}$$

之后, 可以假定

$$\mathscr{A}(T_{12}(1)) = T_{12}(1), \quad \mathscr{A}(T_{21}(-1)) = T_{21}(-1).$$

同时还有

$$\mathscr{A}\begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & A_2 & 0 & B_2 \\ 0 & 0 & 1 & 0 \\ 0 & C_2 & 0 & D_2 \end{pmatrix} = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & A_2 & 0 & B_2 \\ 0 & 0 & 1 & 0 \\ 0 & C_2 & 0 & D_2 \end{pmatrix}.$$

其中

$$\begin{pmatrix} A_2 & B_2 \\ C_2 & D_2 \end{pmatrix} \in Sp_{2\nu-2}(K).$$

因 $Sp_{2\nu}(K)$ 由 $T_{12}(1)$, $T_{21}(-1)$ 和 Π_2 所生成, 因此有 $\mathscr{A}(X) = X$ 对一切 $X \in Sp_{2\nu}(K)$. 所以定理 1 成立.

§4　射影辛对合 (K 的特征数 $\neq 2$)

设 T 为辛矩阵, 以 $\bar{T}$ 表由 T 所诱导出的射影变换. 因 $Sp_{2\nu}(K)$ 的中心只包含 $\pm I$, 故 $T = \bar{T}_1$ 当且仅当 $T = \pm \bar{T}_1$.

定义 1　辛矩阵 T 称为射影辛对合, 如 $T^2 = \gamma I$ 而 $\gamma = 1$ 或 -1. γ 称为 T 的数量因子.

两个辛矩阵 T 和 T_1 称为在 $PSp_{2\nu}(K)$ 中共轭, 如有一辛矩阵 P 存在, 使 $PTP^{-1} = \pm T_1$. 容易证明, 共轭对合有相同的数量因子.

定义 2　数量因子为 $+1$ 的辛对合称为第一类的, 而数量因子为 -1 的辛对合称为第二类或第三类的, 视 -1 是 K 中平方元素与否而定.

我们先研究第一类辛对合. 由 $\{p, q\}$ 辛对合及 $\{q, p\}$ 辛对合组成的第一类辛对合称为 p 对合. 自然可设 $2p \leqslant \nu$. 显然, $PSp_{2\nu}(K)$ 中的第一类对合分成 $\left[\frac{\nu}{2}\right]$ 个共轭 p 对合类.

定理 1　$PSp_{2\nu}(K)$ 中两两交换的 p 对合的最大数等于 $\binom{\nu}{p}$, 如 $p \neq 2\nu$; 而 $\geqslant \frac{1}{2}\binom{\nu}{p}$, 如 $p = \frac{\nu}{2}$.

定理 2　$PSp_{2\nu}(K)$ 中两两交换的 1 对合的最大数永远小于两两交换的 p 对合的最大数, 如 $p > 1$.

这两个定理的证明可仿照第六章 §6 一样来进行, 因而我们将证明略去.

进而研究第二类对合和第三类对合. 自然, 第二类对合和第三类对合不能同时在 $PSp_{2\nu}(K)$ 中出现.

定理 3　设 $-1 = i^2$ 而 $i \in K$. 则 $PSp_{2\nu}(K)$ 中第二类辛对合组成单独一个共

轭元素类. 确切地说, 任一第二类辛对合皆在 $Sp_{2\nu}(K)$ 中共轭于

$$(1)\qquad \begin{pmatrix} iI & \\ & -iI \end{pmatrix}.$$

再设 -1 不是 K 中平方元素, 则每个第三类辛对合在广义辛群之下皆相似于

$$(2)\qquad \begin{pmatrix} 0 & I \\ -I & 0 \end{pmatrix}.$$

【证】 令

$$T = \begin{pmatrix} A & B \\ C & D \end{pmatrix}$$

为辛矩阵, 则

$$T^{-1} = \begin{pmatrix} D' & -B' \\ -C' & A' \end{pmatrix}.$$

如 T 是第二类或第三类对合, 则 $T^{-1} = -T$. 于是

$$T = \begin{pmatrix} A & B \\ C & -A' \end{pmatrix},$$

其中 $B = B'$, $C = C'$ 而 $A^2 + BC = -I$.

现在用归纳法向 ν 来证明本定理.

设 $\nu = 1$. 令

$$T = \begin{pmatrix} a & b \\ c & -a \end{pmatrix}$$

是一个数量因子为 -1 的辛对合. 于是 $a^2 + bc = -1$. 如 $b = 0$, 则 $a^2 = -1$. 我们有

$$\begin{pmatrix} 1 & 0 \\ -\frac{1}{2}a^{-1}c & 1 \end{pmatrix} \begin{pmatrix} a & 0 \\ c & -a \end{pmatrix} \begin{pmatrix} 1 & 0 \\ -\frac{1}{2}a^{-1}c & 1 \end{pmatrix}^{-1} = \begin{pmatrix} a & 0 \\ 0 & -a \end{pmatrix}.$$

如 $a = i$, 定理已经得证. 如 $a = -i$, 则 $-a = i$, 我们有

$$\begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix} \begin{pmatrix} a & 0 \\ 0 & -a \end{pmatrix} \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}^{-1} = \begin{pmatrix} -a & 0 \\ 0 & a \end{pmatrix}.$$

这时定理仍然成立. 其次, 如 $b \neq 0$, 则我们有

$$\begin{pmatrix} 1 & 0 \\ a\ b^{-1} & 1 \end{pmatrix} \begin{pmatrix} a & b \\ c & -a \end{pmatrix} \begin{pmatrix} 1 & 0 \\ a\ b^{-1} & 1 \end{pmatrix}^{-1} = \begin{pmatrix} 0 & b \\ -b^{-1} & 0 \end{pmatrix}.$$

如 $-1 = i^2$, 则

$$\begin{pmatrix} ib^{-1} & 1 \\ -\frac{1}{2} & -\frac{ib}{2} \end{pmatrix}\begin{pmatrix} 0 & b \\ -b^{-1} & 0 \end{pmatrix}\begin{pmatrix} ib^{-1} & 1 \\ -\frac{1}{2} & -\frac{ib}{2} \end{pmatrix}^{-1} = \begin{pmatrix} i & 0 \\ 0 & -i \end{pmatrix},$$

其中 $(ib^{-1})\left(-\frac{ib}{2}\right) - 1\left(-\frac{1}{2}\right) = 1$. 如 -1 不是 K 中平方元素, 则

$$\begin{pmatrix} 1 & 0 \\ 0 & b \end{pmatrix}\begin{pmatrix} 0 & b \\ -b^{-1} & 0 \end{pmatrix}\begin{pmatrix} 1 & 0 \\ 0 & b \end{pmatrix}^{-1} = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}.$$

因此定理当 $\nu = 1$ 时成立.

次设 $\nu > 1$. 假定本定理对于级数 $< 2\nu$ 的辛群已经成立. 令

$$T = \begin{pmatrix} A & B \\ C & -A' \end{pmatrix},$$

$B' = B$, $C' = C$ 而 $A^2 + BC = -I$. 因 B 对称, 有 $\nu \times \nu$ 可逆矩阵 Q 存在, 使

$$QBQ' = \begin{pmatrix} b_1^{(r)} & 0 \\ 0 & 0 \end{pmatrix} = B_1 \text{ (设)},$$

其中 $b_1^{(r)}$ 是非奇异矩阵, $0 \leqslant r \leqslant \nu$. 于是行使辛变换

$$X \to \begin{pmatrix} Q & 0 \\ 0 & Q'^{-1} \end{pmatrix} X \begin{pmatrix} Q & 0 \\ 0 & Q'^{-1} \end{pmatrix}^{-1}$$

之后, 可设

$$B = \begin{pmatrix} b_1^{(r)} & 0 \\ 0 & 0 \end{pmatrix},$$

而 $b_1^{(r)}$ 是非奇异对称阵.

写

$$A = \begin{pmatrix} a_1^{(r)} & a_2^{(r,\nu-r)} \\ a_3^{(\nu-r,r)} & a_4^{(\nu-r)} \end{pmatrix}.$$

因 AB 对称, $a_3 = 0$ 而 $a_1 b_1$ 对称. 注意辛矩阵

$$P = \begin{pmatrix} I & 0 \\ S & I \end{pmatrix}$$

将 T 变为

$$PTP^{-1} = \begin{pmatrix} I & 0 \\ S & I \end{pmatrix} \begin{pmatrix} A & B \\ C & -A' \end{pmatrix} \begin{pmatrix} I & 0 \\ S & I \end{pmatrix}^{-1} = \begin{pmatrix} A - BS & * \\ * & * \end{pmatrix}.$$

如我们选

$$S = \begin{pmatrix} b_1^{-1}a_1 & b_1^{-1}a_2 \\ (b_1^{-1}a_2)' & 0 \end{pmatrix},$$

则 PTP^{-1} 的 A 将取形状

$$\begin{pmatrix} 0 & 0 \\ 0 & a_4 \end{pmatrix}.$$

因 $(A\,B)$ 的秩为 ν, 故 a_4 非奇异. 我们可以一开始就假定

$$A = \begin{pmatrix} 0 & 0 \\ 0 & a_4 \end{pmatrix}, \quad B = \begin{pmatrix} b_1 & 0 \\ 0 & 0 \end{pmatrix}.$$

从 $A^2 + BC = -I$ 推出

$$C = \begin{pmatrix} -b_1^{-1} & 0 \\ 0 & b_2 \end{pmatrix}.$$

因此 T 辛相似于

$$\begin{pmatrix} 0 & 0 & b_1 & 0 \\ 0 & a_4 & 0 & 0 \\ -b_1^{-1} & 0 & 0 & 0 \\ 0 & b_2 & 0 & -a_4' \end{pmatrix},$$

而它是两个数量因子为 -1 的辛对合

$$\begin{pmatrix} 0 & b_1 \\ -b_1^{-1} & 0 \end{pmatrix} \text{和} \begin{pmatrix} a_4 & 0 \\ b_2 & -a_4' \end{pmatrix}$$

的直接和. 因此, 如 $0 < r < \nu$, 从归纳法假设即可推出本定理. 同理, 如 C 的秩既不是 0 也不是 v, 亦可证得定理成立.

现在考查 B 和 C 的秩都是 0 的情形, 这时 $A^2 = -I$. 如 $-1 = i^2$ 在 K 中可解, 则 $(iA)^2 = I$. 这时依第六章定理 6.1, 存在一个非奇异矩阵 P, 使

$$P(iA)P^{-1} = [-1, \cdots, -1, 1, \cdots, 1].$$

于是

$$\begin{pmatrix} P & 0 \\ 0 & P'^{-1} \end{pmatrix}\begin{pmatrix} A & 0 \\ 0 & -A' \end{pmatrix}\begin{pmatrix} P & \\ & P'^{-1} \end{pmatrix}^{-1}$$

$$= -i\begin{pmatrix} [-1,\cdots,-1,1,\cdots,1] & 0 \\ 0 & -[-1,\cdots,-1,1,\cdots,1] \end{pmatrix}.$$

因

$$\begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}\begin{pmatrix} -1 & 0 \\ 0 & 1 \end{pmatrix}\begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}^{-1} = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix},$$

所以 T 在 $Sp_{2\nu}(K)$ 中与 (1) 共轭. 如 -1 不是 K 中平方元素, 则依第六章定理 6.2, 存在一非奇异矩阵 P, 使

$$PAP^{-1} = \begin{pmatrix} 0 & I \\ -I & 0 \end{pmatrix}.$$

(注意这只在 ν 是偶数时才能成立.) 于是

$$\begin{pmatrix} P & 0 \\ 0 & P'^{-1} \end{pmatrix}\begin{pmatrix} A & 0 \\ 0 & -A' \end{pmatrix}\begin{pmatrix} P & 0 \\ 0 & P'^{-1} \end{pmatrix}^{-1} = \begin{pmatrix} 0 & I & & \\ -I & 0 & & \\ & & 0 & I \\ & & -I & 0 \end{pmatrix}.$$

那么

$$\begin{pmatrix} I & 0 & 0 & 0 \\ 0 & 0 & I & 0 \\ 0 & I & 0 & 0 \\ 0 & 0 & 0 & I \end{pmatrix}\begin{pmatrix} 0 & I & & \\ -I & 0 & & \\ & & 0 & I \\ & & -I & 0 \end{pmatrix}\begin{pmatrix} I & 0 & 0 & 0 \\ 0 & 0 & I & 0 \\ 0 & I & 0 & 0 \\ 0 & 0 & 0 & I \end{pmatrix}^{-1} = \begin{pmatrix} 0 & I^{(\nu)} \\ -I^{(\nu)} & 0 \end{pmatrix}.$$

最后, 设 B 的秩为 ν, 则 T 辛相似于

$$\begin{pmatrix} I & \\ B^{-1}A & I \end{pmatrix}\begin{pmatrix} A & B \\ C & -A' \end{pmatrix}\begin{pmatrix} I & \\ B^{-1}A & I \end{pmatrix}^{-1} = \begin{pmatrix} 0 & B \\ -B'^{-1} & 0 \end{pmatrix}.$$

因 B 对称, 有可逆阵 Q 存在, 使

$$QBQ' = [b_1,\cdots,b_\nu].$$

于是我们有

$$\begin{pmatrix} Q & 0 \\ 0 & Q'^{-1} \end{pmatrix}\begin{pmatrix} 0 & B \\ -B^{-1} & 0 \end{pmatrix}\begin{pmatrix} Q & 0 \\ 0 & Q'^{-1} \end{pmatrix}^{-1}$$
$$=\begin{pmatrix} 0 & [b_1,\cdots,b_\nu] \\ [-b_1^{-1},\cdots,-b_\nu^{-1}] & 0 \end{pmatrix},$$

它是 ν 个 2 级辛矩阵

$$\begin{pmatrix} 0 & b_1 \\ -b_1^{-1} & 0 \end{pmatrix},\cdots,\begin{pmatrix} 0 & b_\nu \\ -b_\nu^{-1} & 0 \end{pmatrix}.$$

的直接和. 因之这时定理也成立.

这样, 我们的定理就完全证明了.

§5 射影辛对合的中心化子和 $PSp_{2\nu}(K)$ 的自同构 (K 的特征数 $\neq 2$)

定理 1 p 对合 $\left(p \leqslant \dfrac{\nu}{2}\right)$ 在 $PSp_{2\nu}(K)$ 中的中心化子 $\mathfrak{Z}_1$ 有一个正规群列

$$\mathfrak{Z}_1 \supset \mathfrak{Z}_1' \supset PSp_{2p}(K)\times PSp_{2(\nu-p)}(K) \supset PSp_{2p}(K) \supset \mathfrak{E},$$

其中 $\mathfrak{Z}_1=\mathfrak{Z}_1'$ 或 $\mathfrak{Z}_1:\mathfrak{Z}_1'=2$, 依 $p\neq\dfrac{\nu}{2}$ 或 $p=\dfrac{\nu}{2}$ 而定, 而

$$\mathfrak{Z}_1' : PSp_{2\nu}(K)\times PSp_{2(\nu-p)}(K)=2.$$

【证】 因任意两个 p 对合在 $PSp_{2\nu}(K)$ 中皆共轭, 故只需确定 $\bar{T}_1$ 的中心化子即可, 而

$$T_1=[\underbrace{1,\cdots,1}_{p\text{ 个}},-1,\cdots,-1,\underbrace{1,\cdots,1}_{p\text{ 个}},-1,\cdots,-1].$$

$PSp_{2\nu}(K)$ 中一个元素 $\bar{Q}$ 与 $\bar{T}_1$ 交换当且仅当 $T_1Q=\pm QT_1$. 负号只在 $p=\dfrac{\nu}{2}$ 时才出现. 如果负号出现, 则满足条件 $T_1Q=QT_1$ 的那些 $\bar{Q}$ 组成 $\mathfrak{Z}$ 的一个指数为 2 的正规子群 $\mathfrak{Z}_1'$. 如果负号不出现, 定义 $\mathfrak{Z}_1'=\mathfrak{Z}_1$. 以下来研究群 $\mathfrak{Z}_1'$.

以 Z_1' 表适合条件 $T_1Q=QT_1$ 的那些辛矩阵 Q 所组成的群, 则 Q 必具形状

$$Q=\begin{pmatrix} A_1 & 0 & B_1 & 0 \\ 0 & A_2 & 0 & B_2 \\ C_1 & 0 & D_1 & 0 \\ 0 & C_2 & 0 & D_2 \end{pmatrix}$$

于是

$$Z_1' = Sp_{2p}(K) \times Sp_{2(\nu-p)}(K),$$

因之

$$\mathfrak{Z}_1' : PSp_{2\nu}(K) \times PSp_{2(\nu-p)}(K) = 2.$$

定理 1 证毕.

定理 2 $PSp_{2\nu}(K)$ 中一个第二类辛对合的中心化子 $\mathfrak{Z}_2$ 有一正规群列

$$\mathfrak{Z}_2 \supset \mathfrak{Z}_2' \supset PGL_\nu(K) \supset \mathfrak{E},$$

其中 $\mathfrak{Z}_2 : \mathfrak{Z}_2' = 2, \mathfrak{Z}_2'/PGL_\nu(K)$ 是一个 Abel 群, 它与 K^* 对子群 $\{\pm 1\}$ 的商群同构.

【证】 只要研究 $\bar{T}_2$ 的中心化子, 而

$$T_2 = \begin{pmatrix} iI & \\ & -iI \end{pmatrix}.$$

$PSp_{2\nu}(K)$ 中一个元素 $\bar{Q}$ 与 $\bar{T}_2$ 交换, 当且仅当 $T_2Q = \pm QT_2$. 负号的确出现, 例如

$$\begin{pmatrix} 0 & I \\ -I & 0 \end{pmatrix}\begin{pmatrix} iI & \\ & -iI \end{pmatrix} = -\begin{pmatrix} iI & \\ & -iI \end{pmatrix}\begin{pmatrix} 0 & I \\ -I & 0 \end{pmatrix}.$$

以 $\mathfrak{Z}_2'$ 表那些 $\bar{Q}$ 组成的群而 $T_2Q = QT_2$, 于是 $\mathfrak{Z}_2 : \mathfrak{Z}_2' = 2$. 以 Z_2' 表 $Sp_{2\nu}(K)$ 中适合条件 $T_2Q = QT_2$ 的那些 Q 所组成之群, 则 $\mathfrak{Z}_2' = Z_2'/\{\pm I\}$, 而且 Z_2' 由一切形为

$$Q = \begin{pmatrix} A & 0 \\ 0 & A'^{-1} \end{pmatrix} \quad (A \in GL_\nu(K))$$

的元素组成. 故定理成立.

定理 3 $PSp_{2\nu}(K)$ 中一个第三类对合的中心化子 $\mathfrak{Z}_3$ 有一正规群列

$$\mathfrak{Z}_3 \supset \mathfrak{Z}_3' \supset \mathfrak{E},$$

其中 $\mathfrak{Z}_3 : \mathfrak{Z}_3' = 1$ 或 $2, \mathfrak{Z}_3'$ 是 $Sp_{2\nu}(K)$ 中一个子群的像, 这个子群与一个酉群 $U_\nu(K_0)$ 同构, K_0 是从 K 添加一个 x^2+1 的根而得到的域.

【证】 令

$$T_3 = \begin{pmatrix} 0 & I \\ -I & 0 \end{pmatrix}$$

是一个第三类对合. 以 $\mathfrak{Z}_3'$ 表 $PSp_{2\nu}(K)$ 中那些 $\bar{Q}$ 适合条件 $T_3Q = QT_3$ 者所组成的群, 以 Z_3' 表 $Sp_{2\nu}(K)$ 中适合条件 $T_3Q = QT_3$ 的那些 Q 所组成的群. 则 $\mathfrak{Z}_3 = Z_3'/\{\pm I\}$. Z_3' 由一切形为

$$\begin{pmatrix} A & B \\ -B & A \end{pmatrix}$$

的元素所组成, 其中 $AA' + BB' = I$, AB' 对称. 令 $K_0 = K(i)$, 而 $i^2 + 1 = 0$. 考查对应

$$(1) \qquad \begin{pmatrix} A & B \\ -B & A \end{pmatrix} \to A + iB.$$

易见, $AA' + BB' = I$ 及 AB' 对称, 当且仅当 $(A+iB)\overline{(A+iB)}' = I$. 因此在对应 (1) 之下, Z_3' 与 $U_\nu(K_0)$ 同构. 本定理证毕.

定理 4 在 $PSp_{2\nu}(K)$ 的自同构之下, 1 对合只能映到 1 对合.

【证】 依定理 4.2 知, 在 $PSp_{2\nu}(K)$ 的自同构之下, 1 对合不能映到 p 对合, 如 $p > 1$. 依定理 11 对合在 $PSp_{2\nu}(K)$ 中的中心化子有正规群列, 其中两个商群 $PSp_2(K)$ 和 $PSp_{n-4}(K)$ 是不可换的单群, 除开 $K = F_3$ 这一情形. 而依定理 2 和定理 3, 第二类或第三类对合在 $PSp_{2\nu}(K)$ 中的中心化子有正规群列, 其中顶多有一个商群 $PSL_\nu(K)$ 或 $PTU_\nu(K_0)$ 是不可换的单群. 因此, 1 对合的中心化子不可能和第二类或第三类对合的中心化子同构, 而当 $K = F_3$ 时, 计算一下中心化子的阶亦可得出这一结论. 因此在 $PSp_{2\nu}(K)$ 的自同构之下, 1 对合也不能映到第二类对合或第三类对合.

这样, 在 $PSp_{2\nu}(K)$ 的自同构之下, 1 对合只能映到 1 对合.

仿照定理 3.1 的证明, 可证得

定理 5 $PSp_{2\nu}(K)$ 的任一自同构皆具形状

$$\bar{X} \to \bar{P}\bar{X}^\sigma \bar{P}^{-1},$$

其中 σ 为 K 之自同构, P 为广义辛矩阵.

§6 辛对合 (K 的特征数 $= 2$)

我们现在转入研究特征数 $= 2$ 的域上的辛群的自同构. 从本节起一直到本章之末, 我们都假定域 K 的特征数 $= 2$.

我们仍然从决定辛对合的标准形来开始我们的讨论.

定理 1 每个辛对合都和形状

$$(1) \qquad \begin{pmatrix} I & S \\ 0 & I \end{pmatrix} \quad (S' = S)$$

的一个辛对合辛相似.

【证】 我们向 ν 行使归纳法.

(i) $\nu = 1$. 设

$$T = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$$

是个辛对合, 即

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix}^2 = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix},$$

于是

(2) $$a^2 + bc = d^2 + bc = 1, \quad (a+d)b = (a+d)c = 0.$$

如果 $c = 0$, 则由 (2) 的第一式推出 $a = d = 1$. 于是

$$T = \begin{pmatrix} 1 & b \\ 0 & 1 \end{pmatrix},$$

因此这时引理 1 成立. 现在设 $c \neq 0$, 那么由

$$\begin{pmatrix} 1 & ac^{-1} \\ & 1 \end{pmatrix} \begin{pmatrix} a & b \\ c & d \end{pmatrix} \begin{pmatrix} 1 & ac^{-1} \\ & 1 \end{pmatrix}^{-1} = \begin{pmatrix} 0 & * \\ c & * \end{pmatrix}$$

知, 可以假设 $a = 0$. 于是从 (2) 中第二式 $(a+d)c = 0$ 及 $c \neq 0$ 知 $d = 0$. 于是

$$T = \begin{pmatrix} 0 & b \\ b^{-1} & 0 \end{pmatrix}.$$

那么

$$\begin{pmatrix} b^{-1} & \\ 1 & b \end{pmatrix} \begin{pmatrix} 0 & b \\ b^{-1} & 0 \end{pmatrix} \begin{pmatrix} b^{-1} & \\ 1 & b \end{pmatrix}^{-1} = \begin{pmatrix} 1 & b^{-1} \\ & 1 \end{pmatrix}.$$

因此这时定理也成立.

(ii) $\nu > 1$. 设

$$T = \begin{pmatrix} A & B \\ C & D \end{pmatrix}$$

是一个辛对合. 由 $TFT' = F$ 推出

$$T^{-1} = \begin{pmatrix} D' & B' \\ C' & A' \end{pmatrix}.$$

再由 $T^2 = I$, 即 $T = T^{-1}$ 推出

$$B = B', \quad C = C', \quad A = D'.$$

设 B 的秩为 $r\,(0\leqslant r\leqslant\nu)$, 有 $\nu\times\nu$ 可逆矩阵 Q 存在, 使

$$QBQ^{-1}=\begin{pmatrix} b_1 & 0\\ 0 & 0\end{pmatrix},$$

其中 $b_1=b_1^{(r)}$ 是可逆矩阵. 令

$$T_1=\begin{pmatrix} Q & \\ & Q'^{-1}\end{pmatrix}T\begin{pmatrix} Q & \\ & Q'^{-1}\end{pmatrix}^{-1}=\begin{pmatrix} A_1 & B_1\\ C_1 & D_1\end{pmatrix},$$

则

$$B_1=\begin{pmatrix} b_1 & 0\\ 0 & 0\end{pmatrix}.$$

将 A_1 作与 B_1 同样的分块:

$$A_1=\begin{pmatrix} a_1 & a_2\\ a_3 & a_4\end{pmatrix}.$$

从 $A_1B_1'+B_1A_1'=0$, 即

$$\begin{pmatrix} a_1b_1' & 0\\ a_3b_1' & 0\end{pmatrix}+\begin{pmatrix} b_1a_1' & b_1a_3'\\ 0 & 0\end{pmatrix}=0,$$

推出 $a_3=0$ 及 $b_1a_1'+a_1b_1'=0$. 我们有

$$\begin{pmatrix} I & 0\\ S & I\end{pmatrix}\begin{pmatrix} A_1 & B_1\\ C_1 & A_1'\end{pmatrix}\begin{pmatrix} I & \\ S & I\end{pmatrix}^{-1}=\begin{pmatrix} A_1+B_1S & B_1\\ * & *\end{pmatrix}.$$

因此, 如果取

$$S=\begin{pmatrix} b_1^{-1}a_1 & b_1^{-1}a_2\\ (b_1^{-1}a_2)' & 0\end{pmatrix},$$

则

$$A_1+B_1S=\begin{pmatrix} a_1 & a_2\\ 0 & a_4\end{pmatrix}+\begin{pmatrix} b_1 & 0\\ 0 & 0\end{pmatrix}\begin{pmatrix} b_1^{-1}a_1 & b_1^{-1}a_2\\ (b_1^{-1}a_2)' & 0\end{pmatrix}=\begin{pmatrix} 0 & 0\\ 0 & a_4\end{pmatrix}.$$

置

$$T_2=\begin{pmatrix} I & 0\\ S & I\end{pmatrix}T_1\begin{pmatrix} I & 0\\ S & I\end{pmatrix}=\begin{pmatrix} A_2 & B_2\\ C_2 & D_2\end{pmatrix},$$

则

$$A_2 = \begin{pmatrix} 0 & 0 \\ 0 & a_4 \end{pmatrix}, \quad B_2 = \begin{pmatrix} b_1 & 0 \\ 0 & 0 \end{pmatrix}.$$

将 C_2 作与 A_2, B_2 同样的分块:

$$C_2 = \begin{pmatrix} c_1 & c_2 \\ c_2' & c_4 \end{pmatrix}.$$

从 $BC' + AD' = I$, 即

$$\begin{pmatrix} b_1 & 0 \\ 0 & 0 \end{pmatrix}\begin{pmatrix} c_1 & c_2 \\ c_2' & c_4 \end{pmatrix} + \begin{pmatrix} 0 & 0 \\ 0 & a_4 \end{pmatrix}\begin{pmatrix} 0 & 0 \\ 0 & a_4 \end{pmatrix} = \begin{pmatrix} I & 0 \\ 0 & I \end{pmatrix},$$

推出 $c_2 = 0$. 因此

$$T_2 = \begin{pmatrix} 0 & 0 & b_1 & 0 \\ 0 & a_4 & 0 & 0 \\ c_1 & 0 & 0 & 0 \\ 0 & c_4 & 0 & a_4' \end{pmatrix},$$

它是两个辛矩阵

$$\begin{pmatrix} 0 & b_1 \\ c_1 & 0 \end{pmatrix} \text{和} \begin{pmatrix} a_4 & 0 \\ c_4 & a_4' \end{pmatrix}$$

的直接和. 因 T_2 是对合, 所以这两个辛矩阵也是对合. 因此, 如 $r \neq 0$ 或 $r \neq \nu$, 我们的定理即从归纳法假设推出.

现在研究 $r = \nu$ 的情形, 即 B 可逆的情形. 我们有

$$\begin{pmatrix} I & \\ B^{-1}A & I \end{pmatrix}\begin{pmatrix} A & B \\ C & A' \end{pmatrix}\begin{pmatrix} I & \\ B^{-1}A & I \end{pmatrix}^{-1} = \begin{pmatrix} 0 & B \\ B^{-1} & 0 \end{pmatrix}.$$

因 $B' = B$, 故

$$\begin{pmatrix} B^{-1} & \\ I & B \end{pmatrix}$$

是辛矩阵. 我们有

$$\begin{pmatrix} B^{-1} & \\ I & B \end{pmatrix}\begin{pmatrix} 0 & B \\ B^{-1} & 0 \end{pmatrix}\begin{pmatrix} B^{-1} & \\ I & B \end{pmatrix}^{-1} = \begin{pmatrix} I & B^{-1} \\ & I \end{pmatrix}.$$

因 $B' = B$, 故 $(B^{-1})' = B^{-1}$. 因此这时本定理也成立.

最后研究 $r=0$ 的情形, 即 $B=0$ 的情形. 如果 $C \neq 0$, 则

$$\begin{pmatrix} 0 & I \\ I & 0 \end{pmatrix}\begin{pmatrix} A & \\ C & A' \end{pmatrix}\begin{pmatrix} 0 & I \\ I & 0 \end{pmatrix} = \begin{pmatrix} A' & C \\ & A \end{pmatrix},$$

这就化为 $B \neq 0$ 的情形. 如果 $C=0$, 则

$$T = \begin{pmatrix} A & \\ & A' \end{pmatrix},$$

而 $A^2 = I$. 有 $\nu \times \nu$ 可逆矩阵 Q 存在, 使

$$QAQ^{-1} = \begin{pmatrix} I^{(p)} & I^{(p)} & \\ & I^{(p)} & \\ & & I^{(\nu-2p)} \end{pmatrix},$$

于是

$$\begin{pmatrix} Q & \\ & Q'^{-1} \end{pmatrix} T \begin{pmatrix} Q & \\ & Q'^{-1} \end{pmatrix}^{-1} = \begin{pmatrix} I^{(p)} & I^{(p)} & & & & \\ & I^{(p)} & & & & \\ & & I^{(\nu-2p)} & & & \\ & & & I^{(p)} & & \\ & & & I^{(p)} & I^{(p)} & \\ & & & & & I^{(\nu-2p)} \end{pmatrix}$$

而

$$\begin{pmatrix} I^{(p)} & & & & & \\ & 0 & & & I^{(p)} & \\ & & I^{(\nu-2p)} & & & \\ & & & I^{(p)} & & \\ & I^{(p)} & & & 0 & \\ & & & & & I^{(\nu-2p)} \end{pmatrix}\begin{pmatrix} I^{(p)} & I^{(p)} & & & & \\ & I^{(p)} & & & & \\ & & I^{(\nu-2p)} & & & \\ & & & I^{(p)} & & \\ & & & I^{(p)} & I^{(p)} & \\ & & & & & I^{(\nu-2p)} \end{pmatrix}$$

$$\cdot\begin{pmatrix} I^{(p)} & & & & & \\ & 0 & & & I^{(p)} & \\ & & I^{(\nu-2p)} & & & \\ & & & I^{(p)} & & \\ & I^{(p)} & & & 0 & \\ & & & & & I^{(\nu-2p)} \end{pmatrix} = \begin{pmatrix} I^{(p)} & & & & I^{(p)} & \\ & I^{(p)} & & I^{(p)} & & \\ & & I^{(\nu-2p)} & & & \\ & & & I^{(p)} & & \\ & & & & I^{(p)} & \\ & & & & & I^{(\nu-2p)} \end{pmatrix}$$

因此这时定理 1 也成立.

定理 1 至此完全证毕.

定理 2　如一辛对合 T 与形状 (1) 的一个辛对合辛相似, 则 S 的秩是 T 的辛不变量.

【证】　S 的秩即为 $T-I$ 的秩, 因而是 T 的辛不变量.

定义　如果一个辛对合 T 与形状 (1) 的一个辛对合辛相似, 而 S 的秩为 p, 则 T 称为 p 对合.

定理 3　1 对合在辛变换之下辛相似于形为

$$\begin{pmatrix} I^{(\nu)} & [a,0,\cdots,0] \\ & I^{(\nu)} \end{pmatrix} \quad (a \neq 0),$$

的辛对合, 而在广义辛变换下相似于

$$\begin{pmatrix} I^{(\nu)} & [1,0,\cdots,0] \\ & I^{(\nu)} \end{pmatrix}.$$

这是定理 1 的直接推论.

定理 4　设 T_1 和 T_2 是 $Sp_{2\nu}(K)$ 中两个 1 对合, 而它们的乘积 T_1T_2 的阶为 3, 则可在广义辛变换之下同时变为

$$(3)\qquad \begin{pmatrix} 1 & & 1 & \\ & I^{(\nu-1)} & & 0 \\ & & 1 & \\ & & & I^{(\nu-1)} \end{pmatrix} \text{ 和 } \begin{pmatrix} 1 & & & \\ & I^{(\nu-1)} & & \\ 1 & & 1 & \\ & 0 & & I^{(\nu-1)} \end{pmatrix}.$$

【证】　令 $T_1=I+U, T_2=I+V$. 于是 U,V 的秩皆为 1 而且 $U^2=V^2=0$. 利用 T_1T_2 为 3 阶元素及 $T_1^2=T_2^2=I$ 可推得

$$(UV)^2=UV, \quad (VU)^2=VU.$$

今不妨设 T_1 已经化到 (3) 中前者之形状, 再注意到 $T_2^2=I$, 于是可设

$$U=\begin{pmatrix} 0&0&1&0\\0&0&0&0\\0&0&0&0\\0&0&0&0 \end{pmatrix}, \quad V=\begin{pmatrix} a&x'&b&v'\\u&A&v&B\\c&r'&a&u'\\r&C&x&A' \end{pmatrix},$$

其中 $a, b, c \in K; x', v', u', r'$ 为 $1 \times (\nu - 1)$ 矩阵; A, B, C 为 $\nu - 1$ 阶矩阵且 $B = B'$, $C = C'$. 由

$$VU = \begin{pmatrix} 0 & 0 & a & 0 \\ 0 & 0 & u & 0 \\ 0 & 0 & c & 0 \\ 0 & 0 & r & 0 \end{pmatrix}, \quad (VU)^2 = \begin{pmatrix} 0 & 0 & ac & 0 \\ 0 & 0 & uc & 0 \\ 0 & 0 & c^2 & 0 \\ 0 & 0 & rc & 0 \end{pmatrix}$$

及 $VU = (VU)^2$ 立得 $c^2 = c$. 因之 $c = 1$ 或 0.

今断言 $c = 1$. 否则, 如 $c = 0$, 则 $VU = (VU)^2 = 0$. 另一方面, 由

$$UV = \begin{pmatrix} 0 & r' & a & u' \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \end{pmatrix}, \quad (VU)^2 = 0$$

及 $(UV)^2 = UV$ 推知 $UV = 0$. 这样就推得 $(T_1T_2)^2 = I$, 与假设相矛盾.

于是我们有

$$V = \begin{pmatrix} a & x' & b & v' \\ u & A & v & B \\ 1 & r' & a & u' \\ r & C & x & A' \end{pmatrix}.$$

施行辛变换

$$X \to \begin{pmatrix} 1 & & a & \\ & I & & 0 \\ & & 1 & \\ & & & I \end{pmatrix} X \begin{pmatrix} 1 & & a & \\ & I & & 0 \\ & & 1 & \\ & & & I \end{pmatrix}^{-1},$$

显然它将 U 不变, 而将 V 变为

$$\begin{pmatrix} 0 & * & * & * \\ u & A & * & B \\ 1 & r' & 0 & u' \\ r & C & * & A' \end{pmatrix}.$$

因之可设 $a = 0$. 这样由于 V 的秩为 1, 立得 $x' = 0, b = 0, v' = 0$. 于是

$$V = \begin{pmatrix} 0 & 0 & 0 & 0 \\ u & A & 0 & B \\ 1 & r' & 0 & u' \\ r & C & 0 & A' \end{pmatrix}.$$

再施行辛变换

$$X \to \begin{pmatrix} 1 & & \lambda & u' \\ & I & u & 0 \\ & & 1 & \\ & & & I \end{pmatrix} X \begin{pmatrix} 1 & & \lambda & u' \\ & I & u & 0 \\ & & 1 & \\ & & & I \end{pmatrix}^{-1},$$

其中 $\lambda = u'r$. 显然它将 U 不变, 而将 V 变为

$$\begin{pmatrix} 0 & * & * & * \\ 0 & * & * & * \\ 1 & * & * & * \\ r & * & * & * \end{pmatrix}.$$

于是不妨设 $u = 0$. 因 V 的秩为 1, 故 $A = 0$, $B = 0$. 于是

$$V = \begin{pmatrix} 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 1 & r' & 0 & 0 \\ r & C & 0 & 0 \end{pmatrix}.$$

再施行辛变换

$$X \to \begin{pmatrix} 1 & r' & & \\ & I & & \\ & & 1 & \\ & & r & 1 \end{pmatrix} X \begin{pmatrix} 1 & r' & & \\ & I & & \\ & & 1 & \\ & & r & I \end{pmatrix}^{-1},$$

则它将 U 不变, 而将 V 映为

$$\begin{pmatrix} 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 1 & 0 & 0 & 0 \\ 0 & * & 0 & 0 \end{pmatrix}.$$

于是可设 $r = 0$, 因之 $C = 0$. 这样, 定理 4 就完全证明了.

§7 由一对称矩阵所定义的群 (K 的特征数 $= 2$)

为了研究辛对合的中心化子, 我们需要研究由一个对称矩阵所定义的群. 设 S 为 $n \times n$ 可逆对称矩阵, 以 G 表所有满足条件 $ASA' = S$ 的 $n \times n$ 可逆矩阵 A 所

组成的群. 自然, 合同的对称矩阵给出同构的群, 因此我们先研究 S 在合同下的标准形.

一个 n 维向量 x 称为对 S 而言是迷向的, 如 $xSx'=0$. 两个 n 维向量 x,y 称为对 S 而言是正交的, 如果 $xSy'=0$. 设 P 是一个子空间, 以 P^* 表对 S 而言与 P 中每个向量都正交的向量所组成的子空间. 易见, 如 S 没有迷向向量, 则与 S 合同的矩阵亦然.

定理 1 设 S 为 $n\times n$ 可逆对称矩阵. 则 S 与以下形状的一个矩阵合同:

$$\begin{pmatrix} 0 & I^{(p)} & & & \\ I^{(p)} & 0 & & & \\ & & 0 & I^{(q)} & \\ & & I^{(q)} & C^{(q)} & \\ & & & & D^{(n-2p-2q)} \end{pmatrix}, \tag{1}$$

其中 C 和 D 皆对角形矩阵而且

$$\begin{pmatrix} C & \\ & D \end{pmatrix} \tag{2}$$

是定号的, 即没有迷向向量.

【证】 我们用归纳法向 n 来证明本定理. 当 $n=1$ 时, 定理 1 显然成立. 现在设 $n>1$. 我们分别研究以下诸情形:

(i) 有一对对于 S 迷向的但不正交的向量 x 和 y 存在, 即

$$xSx'=ySy'=0,\quad xSy'\neq 0.$$

我们可以取 $xSy'=1$. 以 $\begin{pmatrix} x \\ y \end{pmatrix}^*$ 表 $\begin{pmatrix} x \\ y \end{pmatrix}$ 对 S 而言的正交补空间, 则

$$\begin{pmatrix} \begin{pmatrix} x \\ y \end{pmatrix} \\ \begin{pmatrix} x \\ y \end{pmatrix}^* \end{pmatrix} S \begin{pmatrix} \begin{pmatrix} x \\ y \end{pmatrix} \\ \begin{pmatrix} x \\ y \end{pmatrix}^* \end{pmatrix}' = \begin{pmatrix} 0 & 1 & \\ 1 & 0 & \\ & & S_1 \end{pmatrix}.$$

于是定理 1 可从归纳法假设推出.

(ii) 没有对于 S 而言的迷向的但不正交的向量对存在.

(ii-1) 有对于 S 而言的迷向向量存在. 设 x 是一个对 S 而言的迷向向量. 可选

取 y 是一个不与 x 正交的向量, 而且可取 $xSy'=1$. 于是

$$\begin{pmatrix} \begin{pmatrix} x \\ y \end{pmatrix} \\ \begin{pmatrix} x \\ y \end{pmatrix}^* \end{pmatrix} S \begin{pmatrix} \begin{pmatrix} x \\ y \end{pmatrix} \\ \begin{pmatrix} x \\ y \end{pmatrix}^* \end{pmatrix}' = \begin{pmatrix} 0 & 1 & \\ 1 & c & \\ & & S_2 \end{pmatrix},$$

其中 $c=ySy'\neq 0$. 根据归纳法假设, 有 $(n-2)\times(n-2)$ 可逆矩阵 P_2, 使

$$P_2S_2P_2' = \begin{pmatrix} 0 & 1 & \\ 1 & C_2 & \\ & & D \end{pmatrix}$$

而

$$\begin{pmatrix} C_2 & \\ & D \end{pmatrix}$$

是定号的. 于是

$$\begin{pmatrix} I^{(2)} & \\ & P_2 \end{pmatrix} S \begin{pmatrix} I^{(2)} & \\ & P_2 \end{pmatrix}' = \begin{pmatrix} 0 & 1 & & & \\ 1 & c & & & \\ & & 0 & I & \\ & & I & C_2 & \\ & & & & D \end{pmatrix}.$$

还需要证明

$$(3)\qquad \begin{pmatrix} c & & \\ & C_2 & \\ & & D \end{pmatrix}$$

是定号的. 实际上, 设有向量 (x,y,z) 具性质

$$(x,y,z)\begin{pmatrix} c & & \\ & C_2 & \\ & & D \end{pmatrix}(x,y,z)'=0,$$

则

$$(0,x,0,y,z)\begin{pmatrix} 0 & 1 & & & \\ 1 & c & & & \\ & & 0 & I & \\ & & I & C_2 & \\ & & & & D \end{pmatrix}(0,x,0,y,z)' = 0.$$

因为 (1, 0, 0, 0, 0) 是迷向的, 而根据假设, 没有迷向的但不正交的向量对存在, 故

$$(1,0,0,0,0)\begin{pmatrix} 0 & 1 & & & \\ 1 & c & & & \\ & & 0 & I & \\ & & I & C_2 & \\ & & & & D \end{pmatrix}(0,x,0,y,z)' = 0.$$

由此推出 $x = 0$. 再从

$$\begin{pmatrix} C_2 & \\ & D \end{pmatrix}$$

的定号性推出 $y = 0, z = 0$. 这就证明了 (3) 是定号的.

(ii-2) 没有对 S 而言的迷向向量存在. 设 x 是一个非 0 向量, 则 x 是非迷向的. 于是

$$\begin{pmatrix} x \\ x^* \end{pmatrix} S \begin{pmatrix} x \\ x^* \end{pmatrix}' = \begin{pmatrix} xSx' & \\ & x^*Sx^{*'} \end{pmatrix},$$

其中 $xSx' \neq 0$. 我们的定理仍从归纳法假设推出, 这时 S 与一定号对角形矩阵合同.

定理 2 设 S 为 $n \times n$ 可逆对称矩阵. 设 S 与 (1) 合同而 (1) 中 (2) 是定号对角形矩阵. 则由 S 定义的群 G 有一正规群列

$$G \supset G_1 \supset G_2 \supset \{I\},$$

其因子群

$$G/G_1 \approx Sp_{2p}(K), \quad G_1/G_2 \approx K^{2pq}, \quad G_2 \approx K^{q(q+1)/2},$$

其中 K^l 表 K 上 l 维向量空间的加群.

【证】 不妨设 S 即为形状 (1). 设 A 为 G 中一元. 将 A 作与 (1) 同样的分

块：

$$A=\begin{pmatrix} A_{11} & A_{12} & A_{13} & A_{14} & A_{15} \\ A_{21} & A_{22} & A_{23} & A_{24} & A_{25} \\ A_{31} & A_{32} & A_{33} & A_{34} & A_{35} \\ A_{41} & A_{42} & A_{43} & A_{44} & A_{45} \\ A_{51} & A_{52} & A_{53} & A_{54} & A_{55} \end{pmatrix}.$$

我们先作以下两个注记：

(i) 将一 n 维行向量 v 作相应的分解

$$v=(v_1,v_2,v_3,v_4,v_5),$$

其中 v_1,v_2 是 p 维向量,v_3,v_4 是 q 维向量, v_5 是 $(n-2p-2q)$ 维向量. 于是

$$vSv'=v_4Cv_4'+v_5Dv_5'.$$

因此, v 是迷向的, 当且仅当 $v_4=0,v_5=0$.

(ii) 设 $(v_1,v_2,v_3,0,0)$ 是一个迷向向量, 我们证明如它与一切迷向向量皆正交, 则 $v_1=v_2=0$. 实际上, 从

$$\begin{aligned}0&=(v_1,v_2,v_3,0,0)S(x_1,x_2,x_3,0,0)'\\&=v_2x_1'+v_1x_2',\end{aligned}$$

对一切 (x_1,x_2,x_3), 推出 $v_1=v_2=0$.

现在设

$$(0,0,v_3,0,0)A=(x_1,x_2,x_3,x_4,x_5).$$

因 $(0,0,v_3,0,0)$ 为迷向向量而且与一切迷向向量皆正交, 故 (x_1,x_2,x_3,x_4,x_5) 亦然, 因此 $x_1=x_2=0$, $x_4=0$, $x_5=0$. 由此推出

(4)
$$A_{31}=0,\quad A_{32}=0,\quad A_{34}=0,\quad A_{35}=0.$$

再设

$$(0,0,0,v_4,v_5)A=(x_1,x_2,x_3,x_4,x_5).$$

于是

$$\begin{aligned}&(0,0,0,v_4,v_5)S(0,0,0,v_4,v_5)'\\=&(x_1,x_2,x_3,x_4,x_5)S(x_1,x_2,x_3,x_4,x_5)',\end{aligned}$$

即

$$v_4Cv_4'+v_5Dv_5'=x_4Cx_4'+x_5Dx_5'.$$

因 (2) 是定号的, 故 $x_4=v_4, x_5=v_5$. 由此推出

(5)
$$A_{44}=I,\quad A_{45}=0,$$
$$A_{54}=0,\quad A_{55}=I.$$

再从 $ASA'=S$ 并利用 (4), (5) 推出

(6)
$$A_{33}=I,\quad A_{14}=0,\quad A_{24}=0.$$

于是 A 取形状

$$A=\begin{pmatrix} A_{11} & A_{12} & A_{13} & 0 & A_{15} \\ A_{21} & A_{22} & A_{23} & 0 & A_{25} \\ 0 & 0 & I & 0 & 0 \\ A_{41} & A_{42} & A_{43} & I & 0 \\ A_{51} & A_{52} & A_{53} & 0 & I \end{pmatrix}$$

再研究 $(0,0,0,0,v_5)$ 在 A 之下的像. 设

$$(0,0,0,0,v_5)A=(x_1,x_2,x_3,0,v_5).$$

我们有

$$(0,0,0,0,v_5)S(y_1,y_2,y_3,0,0)'=0,$$

对一切 y_1,y_2,y_3; 即 $(0,0,0,0,v_5)$ 与一切迷向向量皆正交. 因此

$$(x_1,x_2,x_3,0,v_5)S(y_1,y_2,y_3,0,0)'=0,$$

对一切 y_1,y_2,y_3; 即

$$x_2y_1'+x_1y_2'=0$$

对一切 y_1,y_2. 因此 $x_1=x_2=0$. 于是

(7)
$$A_{51}=A_{52}=0.$$

再从 $ASA'=S$ 推出

(8)
$$A_{15}=A_{25}=0,\ A_{53}=0$$

于是 A 取形状

$$A = \begin{pmatrix} A_{11} & A_{12} & A_{13} & 0 & 0 \\ A_{21} & A_{22} & A_{23} & 0 & 0 \\ 0 & 0 & I & 0 & 0 \\ A_{41} & A_{42} & A_{43} & I & 0 \\ 0 & 0 & 0 & 0 & I \end{pmatrix},$$

其中

$$A_{11}A_{12}' + A_{12}A_{11}' = 0,\ A_{21}A_{22}' + A_{22}A_{21}' = 0,$$
$$A_{11}A_{22}' + A_{12}A_{21}' = I,\ \text{等等}.$$

设 $B \in G$, 于是也有

$$B = \begin{pmatrix} B_{11} & B_{12} & B_{13} & 0 & 0 \\ B_{21} & B_{22} & B_{23} & 0 & 0 \\ 0 & 0 & I & 0 & 0 \\ B_{41} & B_{42} & B_{43} & I & 0 \\ 0 & 0 & 0 & 0 & I \end{pmatrix}.$$

因为

$$AB = \begin{pmatrix} A_{11}B_{11} + A_{12}B_{21} & A_{11}B_{12} + A_{12}B_{22} & * & 0 & 0 \\ A_{21}B_{11} + A_{22}B_{21} & A_{21}B_{12} + A_{22}B_{22} & * & 0 & 0 \\ 0 & 0 & I & 0 & 0 \\ * & * & * & I & 0 \\ 0 & 0 & 0 & 0 & I \end{pmatrix},$$

所以从 G 到 $Sp_{2p}(K)$ 的映射

$$A \to \begin{pmatrix} A_{11} & A_{12} \\ A_{21} & A_{22} \end{pmatrix}$$

是个同态. 同态的核 G_1 由 G 中一切矩阵

$$\begin{pmatrix} I & & A_{13} & & \\ & I & A_{23} & & \\ & & I & & \\ A_{41} & A_{42} & A_{43} & I & \\ & & & & I \end{pmatrix},$$

$$A_{13}' = A_{42},\ A_{23}' = A_{41},$$

$$A_{41}A_{42}' + A_{42}A_{41}' + A_{43} + A_{43}' = 0$$

组成. 又, 映射

$$\begin{pmatrix} I & & A'_{42} & & \\ & I & A'_{41} & & \\ & & I & & \\ A_{41} & A_{42} & A_{43} & I & \\ & & & & I \end{pmatrix} \to \begin{pmatrix} I & & A'_{42} & & \\ & I & A'_{41} & & \\ & & I & & \\ A_{41} & A_{42} & 0 & I & \\ & & & & I \end{pmatrix}$$

是从 G_1 到 G 的一个与 K^{2pq} 同构的子群之上的同态. 同态的核 G_2 由一切形为

$$\begin{pmatrix} I & & & & \\ & I & & & \\ & & I & & \\ & & A_{43} & I & \\ & & & & I \end{pmatrix} \quad (A'_{43} = A_{43})$$

的矩阵组成, 因此 G_2 与 $K^{\frac{q(q+1)}{2}}$ 同构.

定理 2 至此完全证毕.

§8 辛对合的中心化子 (K 的特征数 $=2$)

设 T 是个辛对合, 并设它是个 p 对合. 我们要研究 T 在辛群中的中心化子. 根据定理 1, 不妨设

$$T = \begin{pmatrix} I & S \\ 0 & I \end{pmatrix}$$

而 $S = S'$ 是秩为 p 的对称矩阵. 更不妨设

$$S = \begin{pmatrix} s_1 & 0 \\ 0 & 0 \end{pmatrix},$$

而 $s'_1 = s_1$ 是 $p \times p$ 的可逆对称矩阵. 将 T 的中心化子记作 $\mathfrak{Z}$.

设

$$\Sigma = \begin{pmatrix} A & B \\ C & D \end{pmatrix} \in \mathfrak{Z}.$$

我们有

$$\begin{pmatrix} I & \begin{matrix} s_1 & 0 \\ 0 & 0 \end{matrix} \\ & I \end{pmatrix} = \begin{pmatrix} I & \begin{matrix} s_1 & 0 \\ 0 & 0 \end{matrix} \\ & I \end{pmatrix} \begin{pmatrix} A & B \\ C & D \end{pmatrix},$$

即

$$(1)\quad \begin{pmatrix} A & A\begin{pmatrix} s_1 & 0 \\ 0 & 0 \end{pmatrix} + B \\ C & C\begin{pmatrix} s_1 & 0 \\ 0 & 0 \end{pmatrix} + D \end{pmatrix} = \begin{pmatrix} A + \begin{pmatrix} s_1 & 0 \\ 0 & 0 \end{pmatrix} C & B + \begin{pmatrix} s_1 & 0 \\ 0 & 0 \end{pmatrix} D \\ C & D \end{pmatrix}.$$

将 A, B, C, D 作与 S 同样的分块:

$$A = \begin{pmatrix} a_1 & a_2 \\ a_3 & a_4 \end{pmatrix},$$

$$B = \begin{pmatrix} b_1 & b_2 \\ b_3 & b_4 \end{pmatrix}, \text{ 等等.}$$

比较 (1) 中 (1, 1) 位置和 (2, 2) 位置的矩阵块得

$$\begin{pmatrix} s_1 & 0 \\ 0 & 0 \end{pmatrix} \begin{pmatrix} c_1 & c_2 \\ c_3 & c_4 \end{pmatrix} = 0,$$

$$\begin{pmatrix} c_1 & c_2 \\ c_3 & c_4 \end{pmatrix} \begin{pmatrix} s_1 & 0 \\ 0 & 0 \end{pmatrix} = 0,$$

于是推出

$$c_1 = 0, \quad c_2 = 0, \quad c_3 = 0.$$

再比较 (1) 式中 (1, 2) 位置的矩阵块得

$$\begin{pmatrix} a_1 & a_2 \\ a_3 & a_4 \end{pmatrix} \begin{pmatrix} s_1 & 0 \\ 0 & 0 \end{pmatrix} = \begin{pmatrix} s_1 & 0 \\ 0 & 0 \end{pmatrix} \begin{pmatrix} d_1 & d_2 \\ d_3 & d_4 \end{pmatrix},$$

由此推出

$$a_1 s_1 = s_1 d_1, \quad a_3 = 0, \quad d_2 = 0.$$

于是

$$\Sigma = \begin{pmatrix} a_1 & a_2 & b_1 & b_2 \\ 0 & a_4 & b_3 & b_4 \\ 0 & 0 & s_1^{-1}a_1s_1 & 0 \\ 0 & c_4 & d_3 & d_4 \end{pmatrix}.$$

设

$$\Sigma_1 = \begin{pmatrix} \alpha_1 & \alpha_2 & \beta_1 & \beta_2 \\ 0 & \alpha_4 & \beta_3 & \beta_4 \\ 0 & 0 & s_1^{-1}\alpha_1s_1 & 0 \\ 0 & \gamma_4 & \delta_3 & \delta_4 \end{pmatrix}$$

是 T 的中心化子 $\mathfrak{Z}$ 中的另一元素, 则

$$\Sigma\Sigma_1 = (M\ N),$$

而

$$M = \begin{pmatrix} a_1\alpha_1 & a_1\alpha_2 + a_2\alpha_4 + b_2\gamma_4 \\ 0 & a_4\alpha_4 + b_4\gamma_4 \\ 0 & 0 \\ 0 & c_4\alpha_4 + d_4\gamma_4 \end{pmatrix},$$

$$N = \begin{pmatrix} a_1\beta_1 + a_2\beta_3 + b_1s_1^{-1}\alpha_1s_1 + b_2\delta_3 & a_1\beta_2 + a_2\beta_4 + b_2\beta_4 \\ a_4\beta_3 + b_3s_1^{-1}\alpha_1s_1 + b_4\delta_3 & a_4\beta_4 + b_4\delta_4 \\ (s_1^{-1}a_1s_1)(s_1^{-1}\alpha_1s_1) & 0 \\ c_4\beta_3 + d_3s_1^{-1}a_1s_1 + d_4\delta_3 & c_4\beta_4 + d_4\delta_4 \end{pmatrix},$$

因此

$$\Sigma \to \begin{pmatrix} a_1 & & & \\ & a_4 & & b_4 \\ & & s_1^{-1}a_1s_1 & \\ & c_4 & & d_4 \end{pmatrix}$$

是从 $\mathfrak{Z}$ 到一切形状

$$\begin{pmatrix} a_1 & & & \\ & a_4 & & b_4 \\ & & s_1^{-1}a_1s_1 & \\ & c_4 & & d_4 \end{pmatrix}$$

的辛矩阵所组成的群 $\mathfrak{E}$ 的一个同态, 而同态的核 $\mathfrak{K}$ 由一切形状

$$\begin{pmatrix} I & a_2 & b_1 & b_2 \\ & I & b_2' & \\ & & I & \\ & & a_2' & I \end{pmatrix} \quad (b' = b_1)$$

的辛矩阵组成. 于是

$$\mathfrak{Z}/\mathfrak{K} \approx \mathfrak{E}.$$

设

$$\Pi_1 = \begin{pmatrix} I & a_2 & b_1 & b_2 \\ & I & b_2' & \\ & & I & \\ & & a_2' & I \end{pmatrix} \text{ 和 } \Pi_2 = \begin{pmatrix} I & \alpha_2 & \beta_1 & \beta_2 \\ & I & \beta_2' & \\ & & I & \\ & & \alpha_2' & I \end{pmatrix}$$

和 $\mathfrak{K}$ 中任意二元, 则

$$\Pi_1\Pi_2 = \begin{pmatrix} I & a_2+\alpha_2 & \beta_1+a_2\beta_2'+b_1+b_2\alpha_2' & b_2+\beta_2 \\ & I & b_2'+\beta_2' & \\ & & I & \\ & & a_2'+\alpha_2' & I \end{pmatrix}.$$

因此

$$\begin{pmatrix} I & a_2 & b_1 & b_2 \\ & I & b_2' & \\ & & I & \\ & & a_2' & I \end{pmatrix} \to \begin{pmatrix} I & a_2 & & \\ & I & & \\ & & I & \\ & & a_2' & I \end{pmatrix}$$

是从 $\mathfrak{K}$ 到由一切形状

$$\begin{pmatrix} I & a_2 & & \\ & I & & \\ & & I & \\ & & a_2' & I \end{pmatrix}$$

的辛矩阵所组成的 Abel 群 $\mathfrak{A}$ 的一个同态, 同态的核 $\mathfrak{K}_1$ 由一切形状

$$\begin{pmatrix} I & & b_1 & b_2 \\ & I & b_2' & \\ & & I & \\ & & & I \end{pmatrix} \quad (b_1' = b_1)$$

的辛矩阵组成. 于是

$$\mathfrak{K}/\mathfrak{K}_1 \approx \mathfrak{A}.$$

这样, 我们就得到 $\mathfrak{Z}$ 的一个正规群列

$$\mathfrak{Z} \supset \mathfrak{K} \supset \mathfrak{K}_1 \supset \{1\},$$

而其因子群为

$$\mathfrak{Z}/\mathfrak{K} \approx \mathfrak{C}, \quad \mathfrak{K}/\mathfrak{K}_1 \approx \mathfrak{A}, \quad \mathfrak{K}_1.$$

容易看出, $\mathfrak{A}$ 与 $\mathfrak{K}_1$ 都是 Abel 群. 现在来研究 $\mathfrak{C}$ 的结构. $\mathfrak{C}$ 由一切形状

$$\begin{pmatrix} a_1 & & & \\ & a_4 & & b_4 \\ & & s_1^{-1}a_1s_1 & \\ & c_4 & & d_4 \end{pmatrix}$$

的辛矩阵组成. 显然 $\mathfrak{C}$ 是两个群 $\mathfrak{C}_1$ 和 $\mathfrak{C}_2$ 的直积, 而 $\mathfrak{C}_1$ 由一切形状

$$\begin{pmatrix} a_1 & & & \\ & I & & \\ & & s_1^{-1}a_1s_1 & \\ & & & I \end{pmatrix} \quad (s_1^{-1}a_1s_1 = a_1'^{-1})$$

的辛矩阵组成, 而 $\mathfrak{C}_2$ 由一切形状

$$\begin{pmatrix} I & & & \\ & a_4 & & b_4 \\ & & I & \\ & c_4 & & d_4 \end{pmatrix}$$

的辛矩阵组成. 因此

$$\mathfrak{C}_2 \approx Sp_{2(\nu-p)}(K),$$

而

$$\mathfrak{C}_1 \approx \{a_1 \mid a_1s_1a_1' = s_1\}.$$

根据定理 7.2, 我们知道, $\mathfrak{C}_1$ 有一正规群列, 它的因子群中, 除了可能有一个为 $Sp_{2q}(K)\,(2q \leqslant p)$ 之外, 都是 Abel 群. 因此, 我们证明了

定理 1 p 对合的中心化子有一个正规群列, 它的因子群中除了一个和 $Sp_{2(\nu-p)}(K)$ 同构以及一个可能和 $Sp_{2q}(K)\,(2q \leqslant p)$ 同构之外, 都是 Abel 群.

§9　1 对合的刻画 (K 的特征数 $= 2$)

定理 1　如 $\nu \neq \nu'$, 则 $Sp_{2\nu}(K)$ 不与 $Sp_{2\nu'}(K)$ 同构.

【证】　不妨设 $\nu > \nu'$. 如 K 为有限域, 则 $Sp_{2\nu}(K)$ 和 $Sp_{2\nu'}(K)$ 都是有限群. 因为 $Sp_{2\nu}(K)$ 包有一个子群, 它由一切形状

$$\begin{pmatrix} I^{(\nu-\nu')} & & & \\ & A^{(\nu')} & & B^{(\nu')} \\ & & I^{(\nu-\nu')} & \\ & C^{(\nu')} & & D^{(\nu')} \end{pmatrix}$$

的辛矩阵组成, 而它与 $Sp_{2\nu'}(K)$ 同构, 所以 $Sp_{2\nu}(K):1 > Sp_{2\nu'}(K):1$. 因此 $Sp_{2\nu}(K) \not\approx Sp_{2\nu}(K)$.

现在设 K 是无限域. 我们向 ν 行使归纳法.

(i) $\nu = 2$. 这时 $\nu' = 1$. $Sp_2(K)$ 中任一对合皆辛相似于以下形状的一个对合:

$$\begin{pmatrix} 1 & x \\ 0 & 1 \end{pmatrix},$$

而它的中心化子 $\mathfrak{Z}$ 由一切形状

$$\begin{pmatrix} a & b \\ & a^{-1} \end{pmatrix} \quad (a \in K^*, b \in K)$$

的元素组成. $\mathfrak{Z}$ 有一正规子群 $\mathfrak{N}$, 它由一切形状

$$\begin{pmatrix} 1 & b \\ & 1 \end{pmatrix} \quad (b \in K)$$

的元素组成. 显然, $\mathfrak{Z}/\mathfrak{N} \approx K^*$ 是 Abel 群, 而 $\mathfrak{N}$ 也是 Abel 群. 故 $\mathfrak{Z}$ 是亚 Abel 群 (一群 G 称为亚 Abel 群, 如 G 有一正规群列, 其因子群皆 Abel 群).

但是, 依定理 8.1, $Sp_{2\nu}(K)$ 中的 1 对合的中心化子有一正规群列, 其因子群中有一个是非 Abel 单群 $Sp_{2(\nu-1)}(K)$, 因此 $Sp_{2\nu}(K)$ 的 1 对合的中心化子不是亚 Abel 群.

所以 $Sp_{2\nu}(K) \not\approx Sp_2(K)$.

(ii) 设定理对于 ν 成立. 我们来证明, $Sp_{2(\nu+1)}(K) \not\approx Sp_{2\nu'}(K)$, 如 $\nu' < \nu + 1$. 我们知道, $Sp_{2(\nu+1)}(K)$ 中的 1 对合的中心化子有一个正规群列, 它的因子群中有一

个是单群 $Sp_{2\nu}(K)$. 但 $Sp_{2\nu'}(K)$ 中 p 对合 $(1 \leqslant p \leqslant \nu')$ 的中心化子有一正规群列, 它有一个因子群与 $Sp_{2(\nu'-p)}(K)$ 同构, 而可能有一个因子群与 $Sp_{2q}(K)\,(2q \leqslant p)$ 同构, 而其余的因子群都是 Abel 群. 因 $\nu'-p<\nu, q<\nu$, 故依归纳法假设, $Sp_{2\nu}(K) \not\approx Sp_{2(\nu'-p)}(K), Sp_{2\nu}(K) \not\approx Sp_{2q}(K)$. 因此 $Sp_{2(\nu+1)}(K) \not\approx Sp_{2\nu'}(K)$, 如 $v' < \nu+1$.

定理 2　设 $\nu \geqslant 3$. 则 $Sp_{2\nu}(K)$ 的自同构一定将 1 对合映到 1 对合.

【证】　根据定理 8.1, 我们知道, 1 对合在 $Sp_{2\nu}(K)$ 中的中心化子有一正规群列, 它有一个因子群与 $Sp_{2(\nu-1)}(K)$ 同构; 而 p 对合在 $Sp_{2\nu}(K)$ 中的中心化子有一正规群列, 它有一个因子群与 $Sp_{2(\nu-p)}(K)$ 同构, 可能有一因子群与 $Sp_{2q}(K)(2q \leqslant p)$ 同构, 而其余的因子群皆 Abel 群. 自然有 $\nu-1>\nu-p$, 对一切 $p>1$. 又从 $\nu \geqslant 3$, 因 $2q \leqslant p$, 故也有 $q<\nu-1$. 因此 $Sp_{2(\nu-1)}(K) \not\approx Sp_{2(\nu-p)}(K), Sp_{2(\nu-1)}(K) \not\approx Sp_{2q}(K)$. 因此, 依 Jordan-Hölder-Schreier 定理, 1 对合的中心化子决不与 p 对合的中心化子同构. 所以在 $Sp_{2\nu}(K)$ 的自同构之下, 1 对合只能映到 1 对合. 定理证毕.

以下讨论 $Sp_4(K)$. $Sp_4(K)$ 中只有 1 对合和 2 对合. 我们知道 2 对合 T 皆辛相似于形为

$$\begin{pmatrix} I^{(2)} & S \\ & I^{(2)} \end{pmatrix}$$

的一个对合, 其中 S 是秩为 2 的对称矩阵; 如 S 是交错的, 我们说 T 是非亚 Abel 2 对合; 如 S 有非 0 对角元素, 我们说 T 是亚 Abel 2 对合. 显然, 非亚 Abel 2 对合在 $Sp_4(K)$ 中组成一共轭元素类, 但它们不与亚 Abel 2 对合共轭. 而且, 如 $K \neq F_2$, 则非亚 Abel 2 对合在 $Sp_4(K)$ 中的中心化子是非亚 Abel 群, 它有一正规群列, 有一因子群与单群 $Sp_2(K)$ 同构; 而亚 Abel 2 对合的中心化子是亚 Abel 群.

定理 3　在 $Sp_4(K)$ 的自同构之下, 1 对合不能映到亚 Abel 2 对合.

【证】　如 $K \neq F_2$, 则 1 对合在 $Sp_4(K)$ 中的中心化子 $\mathfrak{Z}$ 有一正规群列, 它有一因子群是单群 $Sp_2(K)$, 因此 $\mathfrak{Z}$ 是非亚 Abel 群. 这就证明了, 1 一对合不能映到亚 Abel 2 对合.

以下设 $K = F_2$. 如在 $Sp_4(F_2)$ 的自同构 $\mathscr{A}$ 之下, 1 对合映到了亚 Abel 2 对合. 依定理 6.4, 不妨设

$$\mathscr{A}\begin{pmatrix} I & \begin{matrix} 1 & 0 \\ 0 & 0 \end{matrix} \\ & I \end{pmatrix} = \begin{pmatrix} I & \begin{matrix} 1 & 0 \\ 0 & 1 \end{matrix} \\ & I \end{pmatrix}$$

及

$$\mathscr{A}\begin{pmatrix} I & \\ \begin{matrix}1&0\\0&0\end{matrix} & I \end{pmatrix} = \begin{pmatrix} I & \\ \begin{matrix}1&0\\0&1\end{matrix} & I \end{pmatrix}.$$

那么

$$J_1 = \begin{pmatrix} I & \begin{matrix}1&0\\0&0\end{matrix} \\ & I \end{pmatrix} \text{ 和 } J_2 = \begin{pmatrix} I & \\ \begin{matrix}1&0\\0&0\end{matrix} & I \end{pmatrix}$$

在 $Sp_4(F_2)$ 中的中心化子 $\mathfrak{Z}_1$ 就映到

$$T_1 = \begin{pmatrix} I & \begin{matrix}1&0\\0&1\end{matrix} \\ & I \end{pmatrix} \text{ 和 } T_2 = \begin{pmatrix} I & \\ \begin{matrix}1&0\\0&1\end{matrix} & I \end{pmatrix}$$

在 $Sp_4(F_2)$ 中的中心化子 $\mathfrak{Z}_2$. 易见, $\mathfrak{Z}_1$ 由一切形如

$$\begin{pmatrix} 1 & & 0 & \\ & a & & b \\ 0 & & 1 & \\ & c & & d \end{pmatrix}, \quad \begin{vmatrix} a & b \\ c & d \end{vmatrix} = 1$$

的矩阵组成, 因而由 6 个元素组成, 可是 $\mathfrak{Z}_2$ 由一切形为

$$\begin{pmatrix} A & 0 \\ 0 & A'^{-1} \end{pmatrix}, \quad \text{而 } AA' = I$$

的元素组成, 因而由 2 个元素组成. 这就得到一个矛盾. 因此这时定理 3 也成立.

定理 4　设 K 是非完全域, 即 K 中至少有一元素 λ, 它不是 K 中元素的平方. 于是在 $Sp_4(K)$ 的自同构之下, 1 对合不能映到非亚 Abel 2 对合.

【证】　设在 $Sp_4(K)$ 的自同构 $\mathfrak{A}$ 之下, 有 1 对合映到了非亚 Abel 2 对合. 依定理 6.4, 不妨设

$$\mathscr{A}\begin{pmatrix} I & \begin{matrix}1&0\\0&0\end{matrix} \\ & I \end{pmatrix} = \begin{pmatrix} I & \begin{matrix}0&1\\1&0\end{matrix} \\ & I \end{pmatrix},$$

$$\mathscr{A}\begin{pmatrix} I & \\ \begin{matrix}1&0\\0&0\end{matrix} & I \end{pmatrix} = \begin{pmatrix} I & \\ \begin{matrix}0&1\\1&0\end{matrix} & I \end{pmatrix}.$$

于是

$$J_1=\begin{pmatrix} I & \begin{matrix}1&0\\0&0\end{matrix} \\ & I\end{pmatrix} \text{ 和 } J_2=\begin{pmatrix} I & \\ \begin{matrix}1&0\\0&0\end{matrix} & I\end{pmatrix}$$

在 $Sp_4(K)$ 中的中心化子 $\mathfrak{Z}_1$ 就映到

$$T_1=\begin{pmatrix} I & \begin{matrix}0&1\\1&0\end{matrix} \\ & I\end{pmatrix} \text{ 和 } T_2=\begin{pmatrix} I & \\ \begin{matrix}0&1\\1&0\end{matrix} & I\end{pmatrix}$$

在 $Sp_4(K)$ 中的中心化子 $\mathfrak{Z}_2$. 易见 $\mathfrak{Z}_1$ 由一切形如

$$\begin{pmatrix} 1 & & 0 & \\ & a & & b \\ 0 & & 1 & \\ & c & & d \end{pmatrix}, \quad \begin{vmatrix} a & b \\ c & d \end{vmatrix}=1$$

的矩阵组成, 而 $\mathfrak{Z}_2$ 由一切形如

$$\begin{pmatrix} \begin{pmatrix} a & b \\ c & d \end{pmatrix} & \\ & \begin{pmatrix} a & b \\ c & d \end{pmatrix}^{\prime -1} \end{pmatrix}, \quad \begin{vmatrix} a & b \\ c & d \end{vmatrix}=1$$

的矩阵组成. $\mathfrak{Z}_2$ 中对合皆非亚 Abel 2 对合, 因而都与 T_1 共轭. 但 $\mathfrak{Z}_1$ 中却包有一个不与 J_1 共轭的对合

$$\begin{pmatrix} I & \begin{matrix}0&0\\0&\lambda\end{matrix} \\ & I\end{pmatrix},$$

这就得到一个矛盾. 因此定理 4 成立.

以下讨论 K 是完全域的情形. 这时确有例表明, $Sp_4(K)$ 的自同构将 1 对合映到非亚 Abel 2 对合 (见 §10). 由于这时 K 中每个元素皆平方元素, 故 $Sp_4(K)$ 中的 1 对合皆共轭. 因此, 如果 $Sp_4(K)$ 的某一自同构将 1 对合映到非亚 Abel 2 对合, 则必将非亚 Abel 2 对合映到 1 对合.

注意, 形如

$$\begin{pmatrix} 1 & \alpha & \beta & \gamma \\ & 1 & \gamma & \\ & & 1 & \\ & & \alpha & 1 \end{pmatrix} \quad (\alpha, \beta, \gamma \text{ 不全为 } 0)$$

的一个对合, 当 $\beta = 0$ 时, 必为非亚 Abel 2 对合; 而当 $\beta \neq 0$ 时, 则为 1 对合, 若 $\alpha = \gamma = 0$; 而为亚 Abel 2 对合, 若 $\alpha \neq 0$ 或 $\gamma \neq 0$.

其次, 设 T 为 1 对合或非亚 Abel 2 对合. 以 C'_T 表一切满足以下条件的辛对合 Q 所组成的集合:

(i) $QT = TQ$;

(ii) Q 为 1 对合或非亚 Abel 2 对合;

(iii) Q 不与 T 共轭.

再以 C''_T 表由所有与 C'_T 中每元皆交换的对合所组成之集合. 于是有

定理 5　设 K 为完全域. 令

$$T_1 = \begin{pmatrix} I^{(2)} & & 1 \\ & 1 & \\ & & I^{(2)} \end{pmatrix}, \quad \begin{pmatrix} I^{(2)} & 1 & \\ & & 0 \\ & & I^{(2)} \end{pmatrix}.$$

于是 C''_{T_1} 由一切形如

$$\begin{pmatrix} 1 & & a & b \\ & 1 & b & c \\ & & 1 & \\ & & & 1 \end{pmatrix} \quad (a, b, c \in K)$$

的元素组成, 而 C''_{J_1} 由一切形如

$$\begin{pmatrix} 1 & \alpha & \beta & \gamma \\ & 1 & \gamma & \\ & & 1 & \\ & & \alpha & 1 \end{pmatrix} \quad (\alpha, \beta, \gamma \in K)$$

的元素组成.

【证】　易见, C'_{T_1} 由一切形如

$$\begin{pmatrix} I^{(2)} & B \\ & I^{(2)} \end{pmatrix}$$

的矩阵组成, 其中 B 是秩为 1 的对称矩阵. 因之, C''_{T_1} 由一切形如

$$\begin{pmatrix} I^{(2)} & \begin{matrix} a & b \\ b & c \end{matrix} \\ & I^{(2)} \end{pmatrix} \quad (a, b, c \in K)$$

的元素组成.

其次, 考虑 C'_{J_1}. 我们断言 C'_{J_1} 由一切形如

(1) $$\begin{pmatrix} 1 & a & & b \\ & 1 & b & \\ & & 1 & \\ & & a & 1 \end{pmatrix} \quad (a, b \in K)$$

的非亚 Abel 2 对合组成. 事实上, 设 $Q \in C'_{J_1}$, 则由 $Q^2 = I$ 及 Q 与 J_1 交换, 可设

$$Q = \begin{pmatrix} 1 & a_2 & b_1 & b_2 \\ & a_4 & b_2 & b_4 \\ & & 1 & \\ & c_4 & a_2 & a_4 \end{pmatrix}.$$

因 $Q^2 = I$, 故有

$$\begin{pmatrix} a_4 & b_4 \\ c_4 & a_4 \end{pmatrix}^2 = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}.$$

如果 $\begin{pmatrix} a_4 & b_4 \\ c_4 & a_4 \end{pmatrix} \neq \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$, 则存在 $\begin{pmatrix} p_1 & p_2 \\ p_3 & p_4 \end{pmatrix} \in SL_2(K)$, 使

$$\begin{pmatrix} p_1 & p_2 \\ p_3 & p_4 \end{pmatrix} \begin{pmatrix} a_4 & b_4 \\ c_4 & a_4 \end{pmatrix} \begin{pmatrix} p_1 & p_2 \\ p_3 & p_4 \end{pmatrix}^{-1} = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix},$$

于是

$$Q^* = \begin{pmatrix} 1 & & 0 & \\ & p_1 & & p_2 \\ 0 & & 1 & \\ & p_3 & & p_4 \end{pmatrix} Q \begin{pmatrix} 1 & & 0 & \\ & p_1 & & p_2 \\ 0 & & 1 & \\ & p_3 & & p_4 \end{pmatrix}^{-1} = \begin{pmatrix} 1 & * & * & * \\ & 1 & * & 1 \\ & & 1 & \\ & & * & 1 \end{pmatrix}$$

是一个 1 对合或亚 Abel 2 对合, 因而 Q 亦然. 这就与 $Q \in C'_{J_1}$ 的假设矛盾. 因之有

$$Q = \begin{pmatrix} 1 & a_2 & b_1 & b_2 \\ & 1 & b_2 & 0 \\ & & 1 & \\ & & a_2 & 1 \end{pmatrix}.$$

又因 Q 是非亚 Abel 2 对合, 故有 $b_1 = 0$. 因此 Q 具有形状 (1). 反之, 形如 (1) 的非亚 Abel 2 对合显然属于 C'_{J_1}. 因之, 我们的断言成立.

经过简单计算可以看出, C''_{J_1} 由一切形如

$$\begin{pmatrix} 1 & \alpha & \beta & \gamma \\ & 1 & \gamma & \\ & & 1 & \\ & & \alpha & 1 \end{pmatrix} \quad (\alpha, \beta, \gamma \in K)$$

的辛对合组成.

§10　$Sp_{2m}(K)$ 的自同构 (K 的特征数 $= 2$)

L. E. Dickson 曾经证明①, 特征数任意的域 K 上的辛群 $Sp_{2m}(K)$ 与一个抽像群 G 同构, 这个群 G 由以下生成元生成:

(0)
$$L_{i\lambda},\ L'_{i\lambda},\ Q_{ij\lambda},\ N_{ij\lambda},\ S_{ij\lambda},$$

其中 λ 跑过 $K, 1 \leqslant i, j \leqslant m$ 而 $i \neq j$; 这组生成元适合下列定义关系:

(1)
$$N_{ij\lambda} = N_{ij\lambda},\ S_{ji\lambda} = S_{ij\lambda};$$

(2) 具不同足码的两个生成元可交换;

(3)
$$(L_{i\lambda}, N_{ij\mu}) = (L_{i\lambda}, Q_{ij\mu}) = (L'_{i\lambda}, Q_{ji\mu}) = (L'_{i\lambda}, S_{ij\mu}) = I;$$

(4)
$$(N_{ij\lambda}, N_{ik\mu}) = (Q_{ij\lambda}, Q_{ik\mu}) = (Q_{ji\lambda}, Q_{ki\mu}) = I;$$

① 见 L. E. Dickson, The abstract form of the abelian linear groups, Quarterly Journal of Pure and Applied Mathematics, vol. **38**(1907), 145～158.

(5) $$(S_{ij\lambda}, S_{ik\mu}) = (N_{ij\lambda}, Q_{ik\mu}) = (S_{ij\lambda}, Q_{ki\mu}) = I;$$

(6) $$(N_{ij\lambda}, S_{ik\mu}) = Q_{jk,-\lambda\mu}, (N_{ij\lambda}, Q_{kj\mu}) = N_{ik,\lambda\mu};$$

(7) $$(S_{ij\lambda}, Q_{ik\mu}) = S_{jk,-\lambda\mu}, (Q_{ij\lambda}, Q_{ki\mu}) = Q_{kj,\lambda\mu};$$

(8) $$(N_{ij\lambda}, Q_{ij\mu}) = L_{i,\lambda\mu}, (S_{ij\lambda}, Q_{ij\mu}) = L'_{j,-2\lambda\mu};$$

(9) $$(Q_{ij\lambda}, L_{j\mu}) = N_{ij,-\lambda\mu}L_{i,-\lambda^2\mu};$$

$$(Q_{ij\lambda}, L'_{i\mu}) = S_{ij,\lambda\mu}L'_{j,-\lambda^2\mu};$$

(10) $$(S_{ij\lambda}, L_{i\mu}) = Q_{ji,\mu\lambda}L'_{j,\lambda^2\mu};$$

$$(N_{ij\lambda}, L'_{i\mu}) = Q_{ij,-\lambda\mu}L'_{j,\lambda^2\mu};$$

(11) $$A_\lambda A_\mu = A_{\lambda+\mu},\ A_0 = I$$

(A_λ 为 (0) 式中任一生成元);

(12) $$L_{i\lambda}L'_{i\mu}L_{i\nu} = L'_{i,\mu\nu\omega^{-1}}L_{i\omega}L'_{i,\lambda\mu\omega^{-1}}$$

(13) $$Q_{ij\lambda}Q_{ji\mu}Q_{ij\nu} = Q_{ji\mu v\omega^{-1}}Q_{ij\omega}Q_{ji\lambda\mu\omega^{-1}};$$

(14) $$S_{ij\lambda}N_{ij\nu}S_{ij\nu} = N_{ij\mu\nu\omega^{-1}}S_{ij\omega}N_{ij\lambda\mu\omega^{-1}};$$

其中 $(A, B) = A^{-1}B^{-1}AB$. 而在 (12)~(14) 式中

$$\omega = \lambda + v + \mu\lambda v \neq 0.$$

L. E. Dickson 在证明中采用了 $Sp_{2m}(K)$ 的如下一组生成元:

$$L_i(\lambda) = \begin{pmatrix} I & 0 \\ \lambda E_{ii} & I \end{pmatrix},\quad L'_i(\lambda) = \begin{pmatrix} I & \lambda E_{ii} \\ 0 & I \end{pmatrix},$$

$$Q_{ij}(\lambda) = \begin{pmatrix} I + \lambda E_{ji} & 0 \\ 0 & I - \lambda E_{ij} \end{pmatrix},$$

$$N_{ij}(\lambda) = \begin{pmatrix} I & 0 \\ \lambda(E_{ij} + E_{ji}) & I \end{pmatrix},$$

$$S_{ij}(\lambda)=\begin{pmatrix} I & \lambda(E_{ij}+E_{ji}) \\ 0 & I \end{pmatrix},$$

其中 $I=I^{(m)}, E_{ij}$ 表 (i,j) 位置为 1 而其余位置为 0 的 $m\times m$ 矩阵, λ 跑过 K. 容易验证, 如将 $L_i(\lambda), L_i'(\lambda), Q_{ij}(\lambda), N_{ij}(\lambda)$ 和 $S_{ij}(\lambda)$ 分别代替 $L_{i\lambda}, L'_{i\lambda}, Q_{ij\lambda}, N_{ij\lambda}$ 和 $S_{ij\lambda}$, 则它们适合关系式 (1)~(14).

现在设 $m=2$ 而 K 是特征数为 2 的完全域. 我们令

$$\tilde{L}_1(\lambda)=\begin{pmatrix} 1 & & & \\ & 1 & & \\ & \lambda^{\frac{1}{2}} & 1 & \\ \lambda^{\frac{1}{2}} & & & 1 \end{pmatrix},\quad \tilde{L}_1'(\lambda)=\begin{pmatrix} 1 & & & \lambda^{\frac{1}{2}} \\ & 1 & \lambda^{\frac{1}{2}} & \\ & & 1 & \\ & & & 1 \end{pmatrix},$$

$$\tilde{L}_2(\lambda)=\begin{pmatrix} 1 & & & \\ \lambda^{\frac{1}{2}} & 1 & & \\ & & 1 & \lambda^{\frac{1}{2}} \\ & & 1 & \end{pmatrix},\quad \tilde{L}_2'(\lambda)=\begin{pmatrix} 1 & \lambda^{\frac{1}{2}} & & \\ & 1 & & \\ & & 1 & \\ & & \lambda^{\frac{1}{2}} & 1 \end{pmatrix},$$

$$\tilde{Q}_{12}(\lambda)=\begin{pmatrix} 1 & & & \\ & 1 & & \\ 0 & & 1 & \\ & \lambda & & 1 \end{pmatrix},\quad \tilde{Q}_{21}(\lambda)=\begin{pmatrix} 1 & & 0 & \\ & 1 & & \lambda \\ & & 1 & \\ & & & 1 \end{pmatrix},$$

$$\tilde{N}_{12}(\lambda)=\tilde{N}_{21}(\lambda)=\begin{pmatrix} 1 & & & \\ & 1 & & \\ \lambda & & 1 & \\ & 0 & & 1 \end{pmatrix},$$

$$\tilde{S}_{12}(\lambda)=\tilde{S}_{21}(\lambda)=\begin{pmatrix} 1 & & \lambda & \\ & 1 & & 0 \\ & & 1 & \\ & & & 1 \end{pmatrix}.$$

容易验证, $\tilde{L}_1(\lambda)$, $\tilde{L}_1'(\lambda)$, $\tilde{L}_2(\lambda)$, $\tilde{L}_2'(\lambda)$, $\tilde{Q}_{12}(\lambda)$, $\tilde{Q}_{21}(\lambda)$, $\tilde{N}_{12}(\lambda)=\tilde{N}_{21}(\lambda)$, $\tilde{S}_{12}(\lambda)=\tilde{S}_{21}(\lambda)$(其中 λ 跑过 K) 这组元素是 $Sp_4(K)$ 的一组生成元, 而且将它们分别代替 $L_{1\lambda}, L'_{1\lambda}, L_{2\lambda}, L'_{2\lambda}, Q_{12\lambda}, Q_{21\lambda}, N_{12\lambda}=N_{21\lambda}, S_{12\lambda}=S_{21\lambda}$, 它们也适合关系式 (1)~(14). 因此我们得到 $Sp_4(K)$ 的一个新型自同构 $\mathscr{A}^*$:

$$L_1(\lambda)=\begin{pmatrix}1&&&\\&1&&\\\lambda&&1&\\&0&&1\end{pmatrix}\rightarrow\tilde{L}_1(\lambda)=\begin{pmatrix}1&&&\\&1&&\\&\lambda^{\frac{1}{2}}&1&\\\lambda^{\frac{1}{2}}&&&1\end{pmatrix},$$

$$L_2(\lambda)=\begin{pmatrix}1&&&\\&1&&\\0&&1&\\&\lambda&&1\end{pmatrix}\rightarrow\tilde{L}_2(\lambda)=\begin{pmatrix}1&&&\\\lambda^{\frac{1}{2}}&1&&\\&&1&\lambda^{\frac{1}{2}}\\&&&1\end{pmatrix},$$

$$L_1'(\lambda)=\begin{pmatrix}1&&\lambda&\\&1&&0\\&&1&\\&&&1\end{pmatrix}\rightarrow\tilde{L}_1'(\lambda)=\begin{pmatrix}1&&&\lambda^{\frac{1}{2}}\\&1&\lambda^{\frac{1}{2}}&\\&&1&\\&&&1\end{pmatrix},$$

$$L_2'(\lambda)=\begin{pmatrix}1&&0&\\&1&&\lambda\\&&1&\\&&&1\end{pmatrix}\rightarrow\tilde{L}_2'(\lambda)=\begin{pmatrix}1&\lambda^{\frac{1}{2}}&&\\&1&&\\&&1&\\&&\lambda^{\frac{1}{2}}&1\end{pmatrix},$$

$$Q_{12}(\lambda)=\begin{pmatrix}1&&&\\\lambda&1&&\\&&1&\lambda\\&&&1\end{pmatrix}\rightarrow\tilde{Q}_{12}(\lambda)=\begin{pmatrix}1&&&\\&1&&\\0&&1&\\&\lambda&&1\end{pmatrix},$$

$$Q_{21}(\lambda)=\begin{pmatrix}1&\lambda&&\\&1&&\\&&1&\\&&\lambda&1\end{pmatrix}\rightarrow\tilde{Q}_{21}(\lambda)=\begin{pmatrix}1&&0&\\&1&&\lambda\\&&1&\\&&&1\end{pmatrix},$$

$$N_{12}(\lambda)=\begin{pmatrix}1&&&\\&1&&\\&\lambda&1&\\\lambda&&&1\end{pmatrix}\rightarrow\tilde{N}_{12}(\lambda)=\begin{pmatrix}1&&&\\&1&&\\\lambda&&1&\\&0&&1\end{pmatrix},$$

$$S_{12}(\lambda)=\begin{pmatrix}1&&&\lambda\\&1&\lambda&\\&&1&\\&&&1\end{pmatrix}\rightarrow\tilde{S}_{12}(\lambda)=\begin{pmatrix}1&&\lambda&\\&1&&0\\&&1&\\&&&1\end{pmatrix},$$

其中 λ 跑过 K.

定理 1　设 K 是特征数为 2 的完全域, 而 $\mathscr{A}$ 是 $Sp_4(K)$ 的一个自同构. 如果 $\mathscr{A}$ 将 1 对合映到非亚 Abel 2 对合, 则 $\mathscr{A}$ 必为以上所定义的 $\mathscr{A}^*$ 和一个形为

$$X \to PX^{\sigma}P^{-1}, \quad X \in Sp_4(K) \tag{15}$$

(其中 σ 为 K 的一个自同构, $P \in Sp_4(K)$) 的自同构之积.

【证】　根据定理 6.4, 不妨设

$$\mathscr{A}(T_1) = J_1, \quad \mathscr{A}(T_2) = J_2, \tag{16}$$

而

$$T_1 = \begin{pmatrix} I & H \\ & I \end{pmatrix}, \quad T_2 = \begin{pmatrix} I & \\ H & I \end{pmatrix},$$

$$J_1 = \begin{pmatrix} & 1 & & \\ I & & & \\ & & & 0 \\ & & I & \end{pmatrix}, \quad J_2 = \begin{pmatrix} & I & & \\ 1 & & & \\ & & & I \\ & & 0 & \end{pmatrix},$$

其中 $H = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$. $\{T_1, T_2\}$ 的中心化子 Γ 由一切形如

$$\begin{pmatrix} \begin{pmatrix} a & b \\ c & d \end{pmatrix} & \\ & \begin{pmatrix} a & b \\ c & d \end{pmatrix}^{\prime -1} \end{pmatrix}, \quad \begin{vmatrix} a & b \\ c & d \end{vmatrix} = 1$$

的元素所组成, 而 $\{J_1, J_2\}$ 的中心化子 Γ' 由一切形如

$$\begin{pmatrix} 1 & & 0 & \\ & \alpha & & \beta \\ 0 & & 1 & \\ & \gamma & & \delta \end{pmatrix}, \quad \begin{vmatrix} \alpha & \beta \\ \gamma & \delta \end{vmatrix} = 1$$

的元素所组成. Γ 的中心化子 Σ 由一切形如

$$\begin{pmatrix} aI & bH \\ cH & dI \end{pmatrix}, \quad 而 \begin{vmatrix} a & b \\ c & d \end{vmatrix} = 1$$

的元素所组成, 而 Γ' 的中心化子 Σ' 由一切形如

$$\begin{pmatrix} \alpha & & \beta & \\ & 1 & & 0 \\ \gamma & & \delta & \\ & 0 & & 1 \end{pmatrix}, \quad 而 \begin{vmatrix} \alpha & \beta \\ \gamma & \delta \end{vmatrix} = 1$$

的元素所组成. 自然有

$$\mathscr{A}(\Sigma) = \Sigma',$$

即

$$\mathscr{A}\begin{pmatrix} aI & bH \\ cH & dI \end{pmatrix} = \begin{pmatrix} \alpha & & \beta & \\ & 1 & & 0 \\ \gamma & & \delta & \\ & 0 & & 1 \end{pmatrix},$$

而

$$\begin{vmatrix} a & b \\ c & d \end{vmatrix} = \begin{vmatrix} \alpha & \beta \\ \gamma & \delta \end{vmatrix} = 1.$$

因此 $\mathscr{A}$ 导出 $SL_2(K)$ 的一个自同构. 有

$$\begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix} = P\begin{pmatrix} a & b \\ c & d \end{pmatrix}^{\sigma} P^{-1},$$

其中 σ 为 K 之自同构而 $P \in GL_2(K)$. 又由 K 中每个元素皆平方元素, 更可设 $P \in SL_2(K)$. 由 (16) 知, 有

$$\begin{pmatrix} 1 & 1 \\ & 1 \end{pmatrix} = P\begin{pmatrix} 1 & 1 \\ & 1 \end{pmatrix}^{\sigma} P^{-1},$$

$$\begin{pmatrix} 1 & \\ 1 & 1 \end{pmatrix} = P\begin{pmatrix} 1 & \\ 1 & 1 \end{pmatrix}^{\sigma} P^{-1}.$$

于是推出 $P = I$. 因此

$$\begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix} = \begin{pmatrix} a & b \\ c & d \end{pmatrix}^{\sigma}.$$

施行 $Sp_4(K)$ 的一个自同构

$$X \to X^{\sigma^{-1}}$$

之后, 可设

$$(17)\qquad \mathscr{A}\begin{pmatrix} aI & bH \\ cH & dI \end{pmatrix} = \begin{pmatrix} a & & b & \\ & 1 & & 0 \\ c & & d & \\ & 0 & & 1 \end{pmatrix},$$

而

$$\begin{vmatrix} a & b \\ c & d \end{vmatrix} = 1.$$

再由

$$\mathscr{A}(\Gamma) = \Gamma',$$

即

$$\mathscr{A}\begin{pmatrix} \begin{pmatrix} a & b \\ c & d \end{pmatrix} & \\ & \begin{pmatrix} a & b \\ c & d \end{pmatrix}^{\prime -1} \end{pmatrix} = \begin{pmatrix} 1 & & 0 & \\ & \alpha & & \beta \\ 0 & & 1 & \\ & \gamma & & \sigma \end{pmatrix}$$

而

$$\begin{vmatrix} a & b \\ c & d \end{vmatrix} = \begin{vmatrix} \alpha & \beta \\ \gamma & \delta \end{vmatrix} = 1,$$

可设

$$\begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix} = P\begin{pmatrix} a & b \\ c & d \end{pmatrix}^{\sigma} P^{-1},$$

其中 σ 为 K 之自同构, 而

$$P = \begin{pmatrix} p_1 & p_2 \\ p_3 & p_4 \end{pmatrix} \in SL_2(K).$$

于是. 施行 $Sp_4(K)$ 的一个形如 (15) 的自同构

$$X \to \begin{pmatrix} 1 & & 0 & \\ & p_1 & & p_2 \\ 0 & & 1 & \\ & P_3 & & p_4 \end{pmatrix}^{-1} X \begin{pmatrix} 1 & & 0 & \\ & p_1 & & p_2 \\ 0 & & 1 & \\ & p_3 & & p_4 \end{pmatrix}$$

之后, 除了 (17) 成立以外, 还可设

$$\mathscr{A}\begin{pmatrix} \begin{pmatrix} a & b \\ c & d \end{pmatrix} & \\ & \begin{pmatrix} a & b \\ c & d \end{pmatrix}^{\prime -1} \end{pmatrix} = \begin{pmatrix} 1 & & 0 & \\ & a^{\sigma} & & b^{\sigma} \\ 0 & & 1 & \\ & c^{\sigma} & & d^{\sigma} \end{pmatrix}, \tag{18}$$

而

$$\begin{vmatrix} a & b \\ c & d \end{vmatrix} = 1.$$

进一步决定 Dickson 所采用的 $Sp_4(K)$ 的那组生成元在 $\mathscr{A}$ 之下的像. 由 (17) 知

$$\mathscr{A}(T_1) = J_1.$$

于是根据定理 9.5 知 $\mathscr{A}$ 将 C''_{T_1} 映到 C''_{J_1} 之上, 因此可设

$$\mathscr{A}\begin{pmatrix} I & \begin{matrix} b & c \\ c & d \end{matrix} \\ & I \end{pmatrix} = \begin{pmatrix} 1 & \alpha & \gamma & \beta \\ & 1 & \beta & \\ & & 1 & \\ & & \alpha & 1 \end{pmatrix}$$

因 $\mathscr{A}$ 将 1 对合映到非亚 Abel 2 对合, 故必有

$$\mathscr{A}\begin{pmatrix} I & \begin{matrix} b & \\ & 0 \end{matrix} \\ & I \end{pmatrix} = \begin{pmatrix} 1 & \alpha & 0 & \beta \\ & 1 & \beta & \\ & & 1 & \\ & & \alpha & 1 \end{pmatrix}.$$

由于

$$\begin{pmatrix} I & \begin{matrix} b & \\ & 0 \end{matrix} \\ & I \end{pmatrix} \text{ 与 } \begin{pmatrix} 1 & 1 & & \\ & 1 & & \\ & & 1 & \\ & & 1 & 1 \end{pmatrix}$$

可换, 故根据 (18) 推知它们的像

$$\begin{pmatrix} 1 & \alpha & & \beta \\ & 1 & \beta & \\ & & 1 & \\ & & \alpha & 1 \end{pmatrix} \text{ 与 } \begin{pmatrix} 1 & & 0 & \\ & 1 & & 1 \\ & & 1 & \\ & & & 1 \end{pmatrix}$$

可换, 于是推出 $\alpha = 0$. 因之, 对任意 $b \in K$, 都有

$$(19)\qquad \mathscr{A}\begin{pmatrix} I & \begin{matrix} b & \\ & 0 \end{matrix} \\ & I \end{pmatrix} = \begin{pmatrix} I & \begin{matrix} & \beta \\ \beta & \end{matrix} \\ & I \end{pmatrix}.$$

类似地, 可推得

$$(20)\qquad \mathscr{A}\begin{pmatrix} I & \begin{matrix} 0 & \\ & b \end{matrix} \\ & I \end{pmatrix} = \begin{pmatrix} 1 & \alpha & & \\ & 1 & & \\ & & 1 & \\ & & \alpha & 1 \end{pmatrix}.$$

由 (19) 和 (20) 推知

$$(21)\qquad \mathscr{A}\begin{pmatrix} I & \begin{matrix} b & \\ & b \end{matrix} \\ & I \end{pmatrix} = \begin{pmatrix} 1 & \alpha & \alpha\beta & \beta \\ & 1 & \beta & \\ & & 1 & \\ & & \alpha & 1 \end{pmatrix}.$$

又由 (17) 有

$$(22)\qquad \mathscr{A}\begin{pmatrix} I & \begin{matrix} & b \\ b & \end{matrix} \\ & I \end{pmatrix} = \begin{pmatrix} 1 & & b & \\ & 1 & & 0 \\ & & 1 & \\ & & & 1 \end{pmatrix}.$$

再考虑到

$$\begin{pmatrix} 1 & & b & b \\ & 1 & b & b \\ & & 1 & \\ & & & 1 \end{pmatrix} = \begin{pmatrix} 1 & & & b \\ & 1 & b & \\ & & 1 & \\ & & & 1 \end{pmatrix}\begin{pmatrix} 1 & & b & \\ & 1 & & b \\ & & 1 & \\ & & & 1 \end{pmatrix}$$

$$= \begin{pmatrix} 1 & & & \\ 1 & 1 & & \\ & & 1 & 1 \\ & & & 1 \end{pmatrix}\begin{pmatrix} 1 & & b & \\ & 1 & & 0 \\ & & 1 & \\ & & & 1 \end{pmatrix}\begin{pmatrix} 1 & & & \\ 1 & 1 & & \\ & & 1 & 1 \\ & & & 1 \end{pmatrix},$$

利用 (18), (19), (21), (22), 就有

$$\mathscr{A}\begin{pmatrix}1 & & b & b\\ & 1 & b & b\\ & & 1 & \\ & & & 1\end{pmatrix}=\begin{pmatrix}1 & & b & \\ & 1 & & 0\\ & & 1 & \\ & & & 1\end{pmatrix}\begin{pmatrix}1 & \alpha & \alpha\beta & \beta\\ & 1 & \beta & \\ & & 1 & \\ & & \alpha & 1\end{pmatrix}$$

$$=\begin{pmatrix}1 & & & \\ & 1 & & \\ & & 1 & \\ & 1 & & 1\end{pmatrix}\begin{pmatrix}1 & & & \beta\\ & 1 & \beta & \\ & & 1 & \\ & & & 1\end{pmatrix}\begin{pmatrix}1 & & & \\ & 1 & & \\ & & 1 & \\ & 1 & & 1\end{pmatrix}.$$

由此推出 $\alpha=\beta=b^{\frac{1}{2}}$. 因此我们有

$$\mathscr{A}\begin{pmatrix}1 & & \lambda & \\ & 1 & & 0\\ & & 1 & \\ & & & 1\end{pmatrix}=\begin{pmatrix}1 & & & \lambda^{\frac{1}{2}}\\ & 1 & \lambda^{\frac{1}{2}} & \\ & & 1 & \\ & & & 1\end{pmatrix}, \tag{23}$$

$$\mathscr{A}\begin{pmatrix}1 & & 0 & \\ & 1 & & \lambda\\ & & 1 & \\ & & & 1\end{pmatrix}=\begin{pmatrix}1 & \lambda^{\frac{1}{2}} & & \\ & 1 & & \\ & & 1 & \\ & & \lambda^{\frac{1}{2}} & 1\end{pmatrix}, \tag{24}$$

对任意 $\lambda\in K$. 再由

$$\begin{pmatrix}1 & & & \\ & 1 & & \\ \lambda & & 1 & \\ & 0 & & 1\end{pmatrix}=\begin{pmatrix} & H\\ H & \end{pmatrix}\begin{pmatrix}1 & & 0 & \\ & 1 & & \lambda\\ & & 1 & \\ & & & 1\end{pmatrix}\begin{pmatrix} & H\\ H & \end{pmatrix}$$

及 (17), (24) 推出

$$\mathscr{A}\begin{pmatrix}1 & & & \\ & 1 & & \\ \lambda & & 1 & \\ & 0 & & 1\end{pmatrix}=\begin{pmatrix}1 & & & \\ & 1 & & \\ & \lambda^{\frac{1}{2}} & 1 & \\ \lambda^{\frac{1}{2}} & & & 1\end{pmatrix}. \tag{25}$$

同样, 由

$$\begin{pmatrix} 1 & & & \\ & 1 & & \\ 0 & & 1 & \\ & \lambda & & 1 \end{pmatrix} = \begin{pmatrix} & H \\ H & \end{pmatrix} \begin{pmatrix} 1 & & \lambda & \\ & 1 & & 0 \\ & & 1 & \\ & & & 1 \end{pmatrix} \begin{pmatrix} & H \\ H & \end{pmatrix}$$

及 (17), (23) 推出

$$\mathscr{A} \begin{pmatrix} 1 & & & \\ & 1 & & \\ 0 & & 1 & \\ & \lambda & & 1 \end{pmatrix} = \begin{pmatrix} 1 & & & \\ \lambda^{\frac{1}{2}} & 1 & & \\ & & 1 & \lambda^{\frac{1}{2}} \\ & & & 1 \end{pmatrix}. \tag{26}$$

最后, 由

$$\begin{pmatrix} a & & & \\ & a^{-1} & & \\ & & a^{-1} & \\ & & & a \end{pmatrix} \begin{pmatrix} 1 & & \lambda & \\ & 1 & & 0 \\ & & 1 & \\ & & & 1 \end{pmatrix} \begin{pmatrix} a & & & \\ & a^{-1} & & \\ & & a^{-1} & \\ & & & a \end{pmatrix}^{-1} = \begin{pmatrix} 1 & & a^2\lambda & \\ & 1 & & 0 \\ & & 1 & \\ & & & 1 \end{pmatrix}$$

及 (18), (23) 得

$$\begin{pmatrix} 1 & & & \\ & a^{\sigma} & & \\ & & 1 & \\ & & & (a^{\sigma})^{-1} \end{pmatrix} \begin{pmatrix} 1 & & & \lambda^{\frac{1}{2}} \\ & 1 & \lambda^{\frac{1}{2}} & \\ & & 1 & \\ & & & 1 \end{pmatrix} \begin{pmatrix} 1 & & & \\ & a^{\sigma} & & \\ & & 1 & \\ & & & (a^{\sigma})^{-1} \end{pmatrix}^{-1} = \begin{pmatrix} 1 & & & a\lambda^{\frac{1}{2}} \\ & 1 & a\lambda^{\frac{1}{2}} & \\ & & 1 & \\ & & & 1 \end{pmatrix},$$

由此推出 $a^{\sigma}=a$. 因此 σ 为 K 的单位自同构, 而 (18) 化为

$$\mathscr{A}\begin{pmatrix}\begin{pmatrix}a&b\\c&d\end{pmatrix}&\\&\begin{pmatrix}a&b\\c&d\end{pmatrix}^{\prime-1}\end{pmatrix}=\begin{pmatrix}1&&0&\\&a&&b\\0&&1&\\&c&&d\end{pmatrix}. \tag{27}$$

注意到 (23), (24), (25), (26), (27) 和 (17), 就有

$$\mathscr{A}=\mathscr{A}^{*}.$$

因此定理 1 成立.

定理 2 设 K 是特征数为 2 的域. 如 $m\neq 2$ 或 $m=2$ 而 K 是非完全域, 则 $Sp_{2m}(K)$ 的自同构必为形状

$$X\to PX^{\sigma}P^{-1}\quad (X\in Sp_{2m}(K)), \tag{28}$$

其中 σ 为 K 之自同构, 而 P 为广义辛矩阵. 在 $m=2$ 而 K 为完全域的情形, $Sp_4(K)$ 的自同构或为形状 (28), 或为以上定义的自同构 $\mathscr{A}^{*}$ 与形为 (28) 的一个自同构之积.

【证】 设 $\mathscr{A}$ 为 $Sp_{2m}(K)$ 的一个自同构. 在 $m=2$ 而 K 为完全域时, 如 $\mathscr{A}$ 将 1 对合映到非亚 Abel 2 对合, 我们的定理由定理 1 推出. 在剩下来需要讨论的情形中, 根据定理 9.2, 9.3 和 9.4, $Sp_{2m}(K)$ 的自同构 $\mathscr{A}$ 必将 1 对合映到 1 对合. 已知当 $m=1$ 时本定理成立, 今对 m 施行归纳法来证明本定理.

由定理 6.4, 可设

$$\mathscr{A}(J_1)=J_1,\quad \mathscr{A}(J_2)=J_2, \tag{29}$$

而

$$J_1=\begin{pmatrix}1&&1&\\&I^{(m-1)}&&0\\&&1&\\&&&I^{(m-1)}\end{pmatrix},$$

$$J_2=\begin{pmatrix}1&&&\\&I^{(m-1)}&&\\1&&1&\\&0&&I^{(m-1)}\end{pmatrix}$$

$\{J_1, J_2\}$ 的中心化子 Σ 由一切形如

$$\begin{pmatrix} 1 & & 0 & \\ & A_1 & & B_1 \\ 0 & & 1 & \\ & C_1 & & D_1 \end{pmatrix}, \quad \begin{pmatrix} A_1 & B_1 \\ C_1 & D_1 \end{pmatrix} \in Sp_{2(m-1)}(K)$$

的辛矩阵组成. 因之, Σ 与 $Sp_{2(m-1)}(K)$ 同构. 自然有 $\mathscr{A}(\Sigma) = \Sigma$, 因此, $\mathscr{A}$ 诱导出 $Sp_{2(m-1)}(K)$ 的一个自同构 $\mathscr{A}_1$. 依归纳法假设, 可设

$$\mathscr{A}_1 \begin{pmatrix} A_1 & B_1 \\ C_1 & D_1 \end{pmatrix} = Q \begin{pmatrix} A_1 & B_1 \\ C_1 & D_1 \end{pmatrix}^{\sigma} Q^{-1},$$

对一切

$$\begin{pmatrix} A_1 & B_1 \\ C_1 & D_1 \end{pmatrix} \in Sp_{2(m-1)}(K),$$

其中 σ 为 K 之自同构, 而 Q 为 $2(m-1) \times 2(m-1)$ 广义辛矩阵. 可以写

$$Q = \begin{pmatrix} Q_1 & Q_2 \\ Q_3 & Q_4 \end{pmatrix} \begin{pmatrix} I^{(m-1)} & \\ & \lambda I^{(m-1)} \end{pmatrix} \quad (\lambda \in K,\ \lambda \neq 0),$$

其中 $\begin{pmatrix} Q_1 & Q_2 \\ Q_3 & Q_4 \end{pmatrix}$ 为 $2(m-1) \times 2(m-1)$ 辛矩阵. 令

$$Q^* = \begin{pmatrix} 1 & & 0 & \\ & Q_1 & & Q_2 \\ 0 & & 1 & \\ & Q_3 & & Q_4 \end{pmatrix} \begin{pmatrix} I^{(m)} & \\ & \lambda I^{(m)} \end{pmatrix},$$

则 Q^* 为 $2m$ 阶广义辛矩阵. 使 $\mathscr{A}$ 承受形为 (14) 的自同构

$$X \to (Q^{*-1} X Q^*)^{\sigma^{-1}}$$

之后, 可以设

$$\mathscr{A} \begin{pmatrix} 1 & & 0 & \\ & A_1 & & B_1 \\ 0 & & 1 & \\ & C_1 & & D_1 \end{pmatrix} = \begin{pmatrix} 1 & & 0 & \\ & A_1 & & B_1 \\ 0 & & 1 & \\ & C_1 & & D_1 \end{pmatrix}, \tag{30}$$

对一切

$$\begin{pmatrix} A_1 & B_1 \\ C_1 & D_1 \end{pmatrix} \in Sp_{2(m-1)}(K).$$

考查 Σ 在 $Sp_{2m}(K)$ 中的中心化子 Σ'. Σ' 由一切形如

$$\begin{pmatrix} a & & b & \\ & I & & 0 \\ c & & d & \\ & 0 & & I \end{pmatrix}, \quad \begin{vmatrix} a & b \\ c & d \end{vmatrix} = 1$$

的元素所组成. 由于 $\mathscr{A}(\Sigma') = \Sigma'$, 而 Σ' 与 $SL_2(K)$ 同构, $\mathscr{A}$ 就诱导出 $SL_2(K)$ 的一个自同构 $\mathscr{A}_2$:

$$\mathscr{A}_2 \begin{pmatrix} a & b \\ c & d \end{pmatrix} = P \begin{pmatrix} a & b \\ c & d \end{pmatrix}^{\tau} P^{-1},$$

其中 τ 为 K 之自同构, 而 $P \in GL_2(K)$. 写

$$P = \begin{pmatrix} p_1 & p_2 \\ p_3 & p_4 \end{pmatrix} \begin{pmatrix} p & \\ & 1 \end{pmatrix},$$

其中 $\begin{pmatrix} p_1 & p_2 \\ p_3 & p_4 \end{pmatrix} \in SL_2(K), p \in K, p \neq 0$. 令

$$P^* = \begin{pmatrix} p_1 & & p_2 & \\ & I^{(m-1)} & & 0 \\ p_3 & & p_4 & \\ & 0 & & I^{(m-1)} \end{pmatrix},$$

即使 $\mathscr{A}$ 承受一个形如 (14) 的自同构

$$X \to P^{*-1} X P^*$$

之后, 除了 (30) 以外, 还可假定

$$\mathscr{A} \begin{pmatrix} a & & b & \\ & I & & 0 \\ c & & d & \\ & 0 & & I \end{pmatrix} = \begin{pmatrix} a^{\tau} & & pb^{\tau} & \\ & I & & 0 \\ p^{-1}c^{\tau} & & d^{\tau} & \\ & 0 & & I \end{pmatrix}. \tag{31}$$

令 Δ 为一切如下元素所组成之集:

$$\begin{pmatrix} I & [b_1, b_2, \cdots, b_m] \\ & I \end{pmatrix},$$

其中 $[b_1, b_2, \cdots, b_m]$ 表一对角矩阵, 主对角线上元素依序为 $b_1, b_2, \cdots, b_m$. 由 (30) 及 (31) 知, $\mathscr{A}(\Delta) = \Delta$. 今考虑 Δ 的中心化子 Ω. 容易证明, Ω 由一切如下形状的对合所组成:

$$\begin{pmatrix} I & S \\ & I \end{pmatrix} \quad (S' = S).$$

由 $\mathscr{A}(\Omega) = \Omega$, 可设

$$\mathscr{A}\begin{pmatrix} I & S \\ & I \end{pmatrix} = \begin{pmatrix} I & S^* \\ & I \end{pmatrix}, \quad 对一切\ S' = S, \tag{32}$$

其中 S^* 自然也是对称矩阵. 类似地, 以 Ω' 表一切如下形状的对合所组成之集:

$$\begin{pmatrix} I & \\ R & I \end{pmatrix} \quad (R' = R),$$

则也有 $\mathscr{A}(\Omega') = \Omega'$, 故可设

$$\mathscr{A}\begin{pmatrix} I & \\ R & I \end{pmatrix} = \begin{pmatrix} I & \\ R^{**} & I \end{pmatrix}, \quad 对一切\ R' = R, \tag{33}$$

其中 R^{**} 也是对称矩阵.

今考虑将 Ω 和 Ω' 各自变到它们自身之中的那些元素组成之群 Γ, 易证 Γ 由一切形为

$$\begin{pmatrix} A & 0 \\ 0 & A'^{-1} \end{pmatrix} \quad (A \in GL_m(K))$$

的元素组成, 于是有 $\mathscr{A}(\Gamma) = \Gamma$.

考查

$$T_{12} = \begin{pmatrix} 1 & 1 & & & & \\ & 1 & & & & \\ & & I & & & \\ & & & 1 & & \\ & & & 1 & 1 & \\ & & & & & I \end{pmatrix}$$

在 $\mathscr{A}$ 之下的像. 因 $T_{12}\in\Gamma$, 故 $\mathscr{A}(T_{12})\in\Gamma$. 如 $m\neq 3$ 或 $m=3$ 而 $K\neq F_2$, 因 T_{12} 与一切形如

$$\begin{pmatrix} I^{(2)} & & & \\ & A & & \\ & & I^{(2)} & \\ & & & A'^{-1} \end{pmatrix} \quad (A\in GL_{m-2}(K))$$

的矩阵交换, 也与一切形如

$$\begin{pmatrix} I & \begin{matrix}\lambda & \\ & 0\end{matrix} \\ & I \end{pmatrix} \quad (\lambda\in K)$$

的矩阵交换, 而且 $T_{12}^2=I$, 故有

$$\mathscr{A}(T_{12})=\begin{pmatrix} 1 & t & & & & \\ & 1 & & & & \\ & & I^{(m-2)} & & & \\ & & & 1 & & \\ & & & t & 1 & \\ & & & & & I^{(m-2)} \end{pmatrix} \quad (t\in K, t\neq 0).$$

如 $m=3$ 而 $K=F_2$. 因 T_{12} 与

$$T_{32}=\begin{pmatrix} 1 & & & & & \\ & 1 & & & & \\ & 1 & 1 & & & \\ & & & 1 & & \\ & & & & 1 & 1 \\ & & & & & 1 \end{pmatrix} \quad 及 \quad T=\begin{pmatrix} 1 & & & 1 & & \\ & 1 & & & 0 & \\ & & 1 & & & 0 \\ & & & 1 & & \\ & & & & 1 & \\ & & & & & 1 \end{pmatrix}$$

交换, 而 $\mathscr{A}(T_{32})=T_{32}, \mathscr{A}(T)=T$, 故

$$\mathscr{A}(T_{12})=\begin{pmatrix} 1 & \lambda & & & & \\ & 1 & & & & \\ & \mu & 1 & & & \\ & & & 1 & & \\ & & & \lambda & 1 & \mu \\ & & & & & 1 \end{pmatrix}.$$

我们考虑元素

$$T_{23}=\begin{pmatrix}1&&&&&\\&1&1&&&\\&&1&&&\\&&&1&&\\&&&&1&\\&&&&1&1\end{pmatrix}.$$

$\mathscr{A}(T_{23})=T_{23}$, 而 $T_{12}T_{23}$ 为 4 阶元素, 故 $\mathscr{A}(T_{12})T_{23}$ 也为 4 阶元素, 由此推出 $\mu=0$. 因此有

$$\mathscr{A}(T_{12})=\begin{pmatrix}1&t&&&&\\&1&&&&\\&&1&&&\\&&&1&&\\&&&t&1&\\&&&&&1\end{pmatrix}\quad(t\in K,t\neq 0).$$

再考查

$$T_{21}=\begin{pmatrix}1&&&&&\\1&1&&&&\\&&I^{(m-2)}&&&\\&&&1&1&\\&&&&1&\\&&&&&I^{(m-2)}\end{pmatrix}$$

在 $\mathscr{A}$ 之下的像. 根据同样的道理, 再根据

$$(T_{12}T_{21})^3=I,$$

推出

$$\mathscr{A}(T_{21})=\begin{pmatrix}1&&&&&\\t^{-1}&1&&&&\\&&I^{(m-2)}&&&\\&&&1&t^{-1}&\\&&&&1&\\&&&&&I^{(m-2)}\end{pmatrix}.$$

于是使 $\mathscr{A}$ 承受形为 (28) 的自同构

$$X \to \begin{pmatrix} t^{-1} & & & \\ & I^{(m-1)} & & \\ & & t & \\ & & & I^{(m-1)} \end{pmatrix} X \begin{pmatrix} t^{-1} & & & \\ & I^{(m-1)} & & \\ & & t & \\ & & & I^{(m-1)} \end{pmatrix}^{-1}$$

之后, 除了 (30), (31) 之外, 还可假定

$$\mathscr{A}(T_{12}) = T_{12}, \quad \mathscr{A}(T_{21}) = T_{21}. \tag{34}$$

因 $Sp_{2m}(K)$ 由 Σ, T_{12}, T_{21} 生成, 故有 $\mathscr{A}(X) = X$, 对一切 $X \in Sp_{2m}(K)$. 这就证明了定理 2.

附　　记

第一章

本章绝大部分结果是熟知的, 例如可在 van der Waerden, Algebra, I, II. Vierte Auflage, Springer, Berlin, 1955~1959 中找到.

定理 4.1 是华罗庚首先得到的, 见 "华罗庚, On the automorphisms of a sfield, Proc. Nat. Acad. Sci. USA. 35 (1949), 386~389", 以及 "华罗庚, 环之准同构及对射影几何的一应用, 中国科学, 1 (1950)1~6".

§11 的结果也是华罗庚首先得到的, 见 "华罗庚, Some properties of a sfield, Proc. Nat. Acad. Sci. USA. 35 (1949), 533~537", 以及 "华罗庚, On the multiplicative group of a field, Science Record, 3 (1950), 1~6".

第二章

定理 2.2 是华罗庚利用他关于体的半自同构的结果证明的, 见 "华罗庚, 环之准同构及对射影几何的一应用, 中国科学, 1 (1951), 1~6".

定理 2.2 是 L. E. Dickson 首先对于有限域证明的, 见 "L. E. Dickson, Linear Groups, B. G. Teubner, 1901" 一书. 随后有很多人包括 L. E. Dickson 本人在内, 作了推广, 最后, J. Dieudonné 在 "Les déterminants sur un corps non commutatif, Bull. Soc. Math. France, 71(1943), 27~45" 一文中推广到任意体上, 但要求体的中心不是只含两个, 三个或五个元素的域, 这些除外的情形后来又被 J. Dieudonné, 华罗庚和王湘浩独立地解决了, 见 "J. Dieudonné, Compléments à trois articles antérieurs, Bull. Soc. Math. France, 74(1946), 59~68"; "华罗庚, Some properties of a sfield, Proc. Nat. Acad. Sci. USA. 35 (1949), 533~537" 以及 "王湘浩, On the commutator subgroup of a simple algebra, Amer. J. Math., 72 (1950), 323~334". 本书采用了王湘浩的证明.

定理 6.1 和定理 9.1 的证明见 "华罗庚和万哲先, 线性群的自同构与同构, 数学学报, 2(1953), 1~32"; 定理 6.2 和定理 9.2 首先由 O. Scheier 和 van der Waerden 给出了一个证明, 见 "O. Schreier 和 van der Waerden, Die Autmorphismen der projektiven Gruppen, Abh. Math. Sem., Hamburg. Univ., 6(1928), 303~322". 后来华罗庚指出他们的证明有错误并重新给出了一个证明, 见 "华罗庚, On the automorphisms

of the symplectic group over any field, Ann. of Math., 49(1948), 739∼759".

定理 7.1 和定理 8.1 是华罗庚证明的, 见 "华罗庚, Supplement to the paper of Dieudonné on the automorphisms of classical groups, Memoirs Amer. Math. Soc., No. 2, 96∼122".

第三章

体上的行列式是 J. Dieudonné 所定义, 见 "J. Dieudonné, Les déterminants sur un corps non commutatif, Bull. Soc. Math. France, 71(1943), 27∼45".

第五章

本章是根据 "华罗庚, 广义域中方阵之一定理及其应用, 数学学报, 1(1951), 109∼163" 一文编写的, 改写过程中也参考了 "万哲先, 王仰贤, 对 '广义域中方阵之一定理及其应用' 一文的讨论, 数学进展, 5(1962), 325∼332".

当基础体是域时, 定理 8.1 周炜良也用另外的方法得到过, 见 "周炜良, On the geometry of algebraic homogeneous spaces, Ann. of Math., 50(1949), 32∼67". 在这之前, 华罗庚先讨论过基础域是复数域的情形, 见 "华罗庚, Geometry of matrices, I, Trans. Amer. Math. Soc., 51(1945), 441∼481; I_1, 同志, 57(1945), 482∼490; II, 同志, 61(1947), 193∼228; III, 同誌, 61(1947), 229∼255". 在这一系列文章中, 不仅得到了矩阵几何的基本定理, 而且提出了以矩阵为几何对像的一系列研究, 似乎还有不少可以发展的方向.

第六章

定理 3.5 是 L. E. Dickson 首先对有限域证明的, 见 "L. E. Dickson, Linear groups" 一书. 随后 L. E. Dickson 和其他一些人又作了推广, 最后 J. Dieudonné 将它推广到一般体上, 见 "J. Dieudonné, Les déterminants sur un corps non commutatif, Bull. Math. Soc. France, 71(1943), 27∼45"; 本书的证明是新的.

定理 5.1 的证明是 J. Dieudonné 首先发表的, 见 "J. Dieudonné, On the automorphisms of classical groups, Memoirs Amer. Math. Soc., No. 2, 1951"; 但他未能证明 $n = 4$ 的情形. 华罗庚在 "On the automorphisms of the symplectic group over any field, Ann. of Math., 49(1948), 739∼759" 一文中提供了确定典型群自同构的一个方法, 运用那个方法也可确定线性群的自同构, 由于 J. Dieudonné 关于典型群自同构的系统研究已经发表, 华罗庚在 "Supplement to the paper of Dieudonné on the automorphisms of classical groups, Memoirs of Amer. Math. Soc., No. 2(1951), 96∼122" 中发表了 J. Dieudonné 所未能确定其自同构的一些情形, 其中也包括 $SL_4(K)$, (K

的特征数 $\neq 2$). 华罗庚运用他的方法和 I. Reiner 一起确定了整数环上线性群的自同构, 见 "华罗庚和 I. Reiner, Automorphisms of the unimodular group, Trans. Amer. Math. Soc., 71 (1951), 331~348", 并在本书初稿中运用他的方法给出了定理 5.1 的一个证明. 后来万哲先运用这一方法确定了非交换主理想整环上线性群的自同构并将证明作了某些简化, 见 "万哲先, 特征数 $\neq 2$ 的非交换主理想整环上线性群的自同构, 数学学报, 7(1957), 533~573". 本书定理 5.1 采用了上述万哲先文中的证明. 运用华罗庚的方法研究典型群自同构或有关问题的还有严士健, 王仰贤, 应玫茜和 M. Abe 等人.

定理 9.1 的证明是 J. Dieudonné 首先发表的, 见 "J. Dieudonné, On the automorphisms of classical groups"; 但他未能证明 $n = 4$ 的情形, 而后来华罗庚和万哲先在 "线性群的自同构与同构, 数学学报, 2(1953), 1~32" 一文中给出了 $n = 4$ 情形的证明. 本书定理 9.1 的证明则是根据 "万哲先, 关于线性群自同构的一个证明, 数学学报, 11(1961), 380~387" 一文编写的.

第七章

本章是根据 "华罗庚, 哈密尔顿型的推广, 数学学报, 3(1953)12~58" 一文编写的, 编写过程中也参考了 "J. Dieudonné, On the struture of unitary groups, Trans. Amer. Math. Soc., 72(1952), 367~385" 一文. 本章中的具体例子特别是 §11 则是参考 "L. E. Dickson, Linear Groups" 一书以及其他一些文献编写的.

定理 4.1 或与之等价的定理 6.1 首先是由 E. Witt 对于特征数 $\neq 2$ 域上的对称矩阵证明的, 见 "E. Witt, Theorie der quadratischen Formen in beliebigen Körpern, J. reine angew. Math., 176(1937), 31~44".

第八章

定理 4.1 是 L. E. Dickson 首先对有限域证明的, 见 "L. E. Dickson, Linear groups" 一书, 后来华罗庚和 J. Dieudonné 将它推广到任意具对合性反自同构的体上, 见 "华罗庚, 哈密尔顿型的推广, 数学学报, 3(1953), 12~58" 以及 "J. Dieudonné, On the structure of unitary group, Trans. Amer. Math. Soc., 72(1952), 367~385"; 本书的证明是新的, 精神上与第六章定理 3.5 的证明一致.

§5 是根据 "万哲先, 酉群对于它的换位子群的商群的构造, 数学学报, 12(1962), 352~368" 一文编写的.

第九章

定理 1.5 是 E. Cartan 首先对于实数域的情形证明的, 见 "E. Cartan, Leçons

sur la théorie des spineurs, I, Hermann, Paris, 1938", 而 J. Dieudonné 则证明了一般情形, 见 "J. Dieudonné, Sur les groupes classiques, Hermann Paris, 1948".

定理 2.4 和定理 3.4 在本章中用来证明定理 6.1, 但它们本身也有独立的兴趣.

M. Eichler 利用旋范数证明了定理 4.3 对于 $n > 2v > 0$ 的情形也成立, 见 "M. Eichler, Quadratische Formen und orthogonale Gruppen, Springer, Berlin, 1952". 像 $n = 2\nu > 4$ 的情形那样, 完全利用初等的矩阵方法给出 $n > 2\nu > 0$ 的情形的一个证明将是我们期望的.

定理 6.1 是 L. E. Dickson 首先对于有限域证明的, 见 "L. E. Dickson, Linear groups"; 后来他又作了一些推广, 见 "L. E. Dickson, Theory of linear groups in an arbitrary field, Trans. Amer. Math. Soc., 2(1901), 363~394" 及 "L. E. Dickson, Linear groups in an infinite field, Proc. London Math. Soc., 34(1902), 185~205", 而 J. Dieudonné 则在一般情形证明了这个定理. J. Dieudonné 的证明利用了 van der Waerden 关于低维正交群与其他类型的典型群同构的结果, 见 "van der Waerden, Gruppen von linearen Transformationen, Springer, Berlin, 1935", 本书的证明则完全不用这些结果, 精神上与第六章定理 3.5 及第八章定理 4.1 的证明一致.

第十章

C. Arf 在 "Untersuchungen über quadratische Formen in Körpern der Charakteristik 2, I. Journ. reine angew. Math., 183 (1941), 148~167" 一文中首先研究了特征数为 2 的域上的二次型并推广了 Witt 定理 (即本章定理 1.4).

定理 6.4 和定理 7.4 在本章中是用来证明定理 8.1 的, 但它们本身也有独立的兴趣.

定理 8.1 首先是 L. E. Dickson 对于有限域证明的, 见 "L. E. Dickson, Linear groups", 后来他又作了一些推广 (见第九章所引 L. E. Dickson 的论文), 而 J. Dieudonné 则在一般情形证明了这个定理, 见 "J. Dieudonné, Sur les groupes classiques". 和定理 6.1 一样, J. Dieudonné 关于定理 8.1 的证明也运用了 van der Waerden 关于低维正交群与其他类型的典型群同构的结果. 本书建议的证明则不用这些结果.

第十一章

本章主要结果是 J. Dieudonné 首先得到的, 见 "J. Dieudonné, Sur les groups classiques", 但本书的证明却是新的. 特别是定理 6.1 的证明, 精神上与第六章定理 3.5 和第十章定理 8.1 的证明一致.

第十二章

定理 3.1 是华罗庚首先得到的, 见 "华罗庚, On the automorphisms of the symplectic group over any field, Ann. of Math., 49 (1948), 739~759". 本书的证明基本是上述论文的证明, 只是作了某些简化.

定理 10.2 在 $m \neq 2$ 时是 J. Dieudonné 首先证明的, 见 "J. Dieudonné, On the automorphisms of classical groups". 他也讨论了 $m = 2$ 的情形, 但万哲先, 王仰贤在 "On the automorphisms of symplectic groups over any field of characteristic 2, 中国科学, 12 (1963), 289~315" 一文中指出 J. Dieudonné关于 $m = 2$ 这一情形的结论是错误的, 他们改正了这一情形的结论, 并给出定理 10.2 一个新的证明, 本书采用了这个新的证明.

索 引

一画

二画

三画

四画

五画

六画

七画

八画

九画

十画

十一画

十二画

十三画

十四画

十五画

十九画

《华罗庚文集》已出版书目

（按出版时间排序）

1 华罗庚文集数论卷 I 王元 审校 2010 年 5 月
2 华罗庚文集数论卷 II 贾朝华 审校 2010 年 5 月
3 华罗庚文集数论卷 III 王元 潘承彪 贾朝华 审校 2010 年 5 月
4 华罗庚文集代数卷 I 万哲先 审校 2010 年 5 月
5 华罗庚文集多复变函数论卷 I 陆启铿 审校 2010 年 5 月
6 华罗庚文集应用数学卷 I 杨德庄 主编 2010 年 5 月
7 华罗庚文集应用数学卷 I 杨德庄 主编 2010 年 5 月
8 华罗庚文集数论卷 II 待定
9 华罗庚文集多复变函数论卷 待定

(O-3859.0101)

中国科学院华罗庚数学重点实验室丛书

华罗庚文集｜代数卷 I｜


ISBN 978-7-03-027126-6
9 787030 271266 >

销售分类建议：高等数学

定价：98.00元